Notes from the field: XenMobile the road so far

This year started out with numerous XenMobile Projects and I would like to share some insights I got during those projects ;) hope you'll find it useful!

I've started mostly everywhere on a XenMobile 10 Deployment, let it be a single server or cluster format, did a couple of migrations from XenMobile 9 but just leave it at that and say just do 10 ☺ saves you a lot of headache.

When deploying the servers keep in mind that we don't have much to do but deploy the basics, like IP settings, perform cluster options and remote access, pretty straightforward. The caveats I found was on the different hypervisors like time drifts or VM locks. In the latest build an CLI NTP option is back, use it! ShareFile is one of the buggers that is highly susceptible to time drifts when using for example IDP integration. The other issue I found was the time zone of the appliance, make sure those are correct! otherwise fun times ahead with troubleshooting.

When you deploy the first server you get the setup wizard and follow it nicely, don't forget when using a cluster or setting it up you will need to have a valid license server configuration, the grace period is limited I've seen and could give you a cluster that sometimes isn't available, keep that in mind for let's say a POC deployment.

Then you start configuring the basics like APNS certificate, 3rd party certificate for you MDM, User Certificate when using an PKI integration, pretty straightforward still. Just keep in mind that Apple completely relies on the Developer Account which in some organizations are shared with other departments who *cough* accidently remove profiles which we rely on, so that's always an area to investigate.

Android integration is normally done by an always on check-in policy, there is an awesome blog regarding GCM integration which I think is going to be the new default. Give it a look at https://www.citrix.com/blogs/2016/04/08/xenmobile-10-3-how-to-configure-google-cloud-messaging-service/ and also https://developers.google.com/cloud-messaging/ (it's now called FCM)

Everything good to go and then off to the client/server properties and going to create a baseline there, keep in mind this is a setup not the one size fits all settings deployment, test it all with your customers' requirements if it will fit in. Good read for this is XenMobile Security - Understanding the technology used by XenMobile

Client Properties

To change a property, select the property and then click Edit.

Add

Name	Key	Value	Description
Enable Worx PIN Authentication	ENABLE_PASSCODE_AUTH	True	Enable Worx PIN Authentication
Enable User Password Caching	ENABLE_PASSWORD_CACHING	True	Enable User Password Caching
Encrypt secrets using Passcode	ENCRYPT_SECRETS_USING_PASSCODE	True	Encrypt secrets using WorxPin or AD password
Worx PIN Type	PASSCODE_TYPE	Numeric	Worx PIN Type
Worx PIN Strength Requirement	PASSCODE_STRENGTH	Medium	Worx PIN Strength Requirement
Worx PIN Length Requirement	PASSCODE_MIN_LENGTH	5	Worx PIN Length Requirement
Worx PIN Change Requirement	PASSCODE_EXPIRY	90	Worx PIN Change Requirement
Worx PIN History	PASSCODE_HISTORY	10	Worx PIN History
Inactivity Timer	INACTIVITY_TIMER	15	Inactivity Timer
Enable FIPS Mode	ENABLE_FIPS_MODE	false	Enable FIPS Mode

Client Properties

To change a property, select the property and then click Edit.

Add

Name	Key	Value	Description
Disable Logging	DISABLE_LOGGING	false	Disable Logging
Enable Crash Reporting	ENABLE_CRASH_REPORTING	false	Enable Crash Reporting
Send device logs to IT help desk	DEVICE_LOGS_TO_IT_HELP_DESK	false	Send device logs to IT help desk
On failure Use Email to Send device logs to IT help desk	ON_FAILURE_USE_EMAIL	true	On failure Use Email to Send device logs to IT help desk
Enable Touch ID Authentication	ENABLE_TOUCH_ID_AUTH	true	Enable Touch ID Authentication
Enable Google Analytics in WorxHome	ENABLE_WORXHOME_GA	false	Enable Google Analytics in WorxHome
Enable Worx Home CEIP	ENABLE_WORXHOME_CEIP	false	Enable Worx Home CEIP
MDX Container Self Destruct Period	CONTAINER_SELF_DESTRUCT_PERIOD	0	MDX Container Self Destruct Period (days)
Worx PIN maximum attempts	PASSCODE_MAX_ATTEMPTS	5	Worx PIN maximum attempts to unlock apps

Above is a basic setup which uses worx-pin for everything and user entropy enabled for extra security.

Then moving on to the server properties to do the following:

- Netscaler Throttling Inteval change from 30 minutes to 0 regarding client certificates
- Skip the second profile installation on iOS when using 3rd party certificate
- Block rooted and jailbroken devices from enrolling
- Disable the self help portal
- Force mandatory enrollment so MDM/MAM (depends which edition is used)

This looks like:

Server Property	**Default Setting**	**Explanation**
Netscaler Gateway Client Cert Issuing Throttling Interval	30	Change this to 0 so that there is not a 30 minute delay in NSGW or blocking it when there are certificate requests
iOS Device Management Enrollment Install Root CA if Required	True	Change to false when using 3rd party certificate, skips an prompt for the user and improves user experience
Block Enrollment of Rooted Android and Jailbroken iOS Devices	False	Change to true to block enrollment of these type of devices, security experience
Enable Console	True	Change to false to disable the self help portal, could be a security requirement
Enrollment Required	False	Change to true to force MDM/MAM enrollment and not give the user a choice, user experience impact and security

The reason I created this document was specifically after this blog:

https://www.citrix.com/blogs/2016/06/03/xenmobile-optimizations-and-assessment-findings/

so I also have some additions which I saw were being added in some large environments regarding server properties: **(WARNING! Test before implementing in production or consult with Citrix support)**

Server Property	**Default Setting**	**Explanation**
Interval for check deleted Active Directory User	0 zero minutes	Change to your Active Directory Synchronization settings for example 15 minutes
Push Services Heartbeat Interval	6 Hours	Regarding Load to the Database change would be 23 Hours
iOS MDM APNS Connection Pool Size	None	Depends on the usage of iOS devices, more than 100 benefit from a change to 10

Background Deployment	360 Minutes	Android Always On – 1440 instead of the default for reduction of server load
Background Hardware Inventory	360 Minutes	Android Always On – 1440 instead of the default for reduction of server load
Custom key: hibernate.c3p0.max_size=500	200	Scaling above and beyond 30,000 devices regarding connection pool max. size **Key: Custom Key** **Key: hibernate.c3p0.max_size** **Value: 500** **Display name: hibernate.c3p0.max_size=500** **Description: DB connections to SQL** In high load situation changing this to **1000** could benefit very large deployments regarding simultaneously connections.
Custom key: hibernate.c3p0.timeout=30	300 seconds	When deployed on a Database Cluster this could benefit by reducing the idle timeout to 30 seconds. **Key: Custom Key** **Key: hibernate.c3p0.timeout** **Value: 30** **Display name: hibernate.c3p0.timeout=30** **Description: Database idle timeout**
Custom key: auth.ldap.connect.timeout=60000	6000	Compensate slow LDAP responses **Key: Custom Key** **Key: auth.ldap.connect.timeout** **Value: 60000** **Display name: auth.ldap.connect.timeout=6000** **Description: LDAP connection timeout**

Custom key: auth.ldap.read.timeout=60000	6000	Compensate slow LDAP responses **Key: Custom Key** **Key: auth.ldap.read.timeout** **Value: 60000** **Display name:** **auth.ldap.read.timeout=60000** **Description: LDAP read timeout**

The other thing I've seen is that the documentation is constantly being updated regarding the development for XenMobile, so this is definitely your friend:

http://docs.citrix.com/en-us/xenmobile/10/xmob-system-requirements.html

One last thing before closing off all my ranting is when integrating with a Microsoft ADCS solution you might get yourself into trouble when your CA server is in a tiered solution, meaning that the CA and Web enrollment feature are not on the same server, I've got an support case open with Citrix and Microsoft that maybe this can be changed but for now the only solution is to add the web role to the CA which is providing user certificates for your mobility deployment.

Well that's that hope this was helpful and I'll close off with some useful links.

XenMobile: Client Certificate Authentication Cheat Sheet
http://support.citrix.com/article/CTX212665

XenMobile Management Tools
https://xenmobiletools.citrix.com/XenMobileCloudTools-3.0/home/

XenMobile 10.x Deployment Resources
http://support.citrix.com/article/CTX208167

XenMobile POC Cheat Sheet
http://support.citrix.com/article/CTX213658

XenMobile 10.3.5 VPP hotfix
http://support.citrix.com/article/CTX212769

Android 6 Encryption Error when starting Worx applications
http://support.citrix.com/article/CTX213353

And the last update on Android Marshmellow also keep in mind that encryption is enabled by default regarding to your MDM policies for previous Android devices and/or they have encryption policies enabled in XenMobile those will then fail.