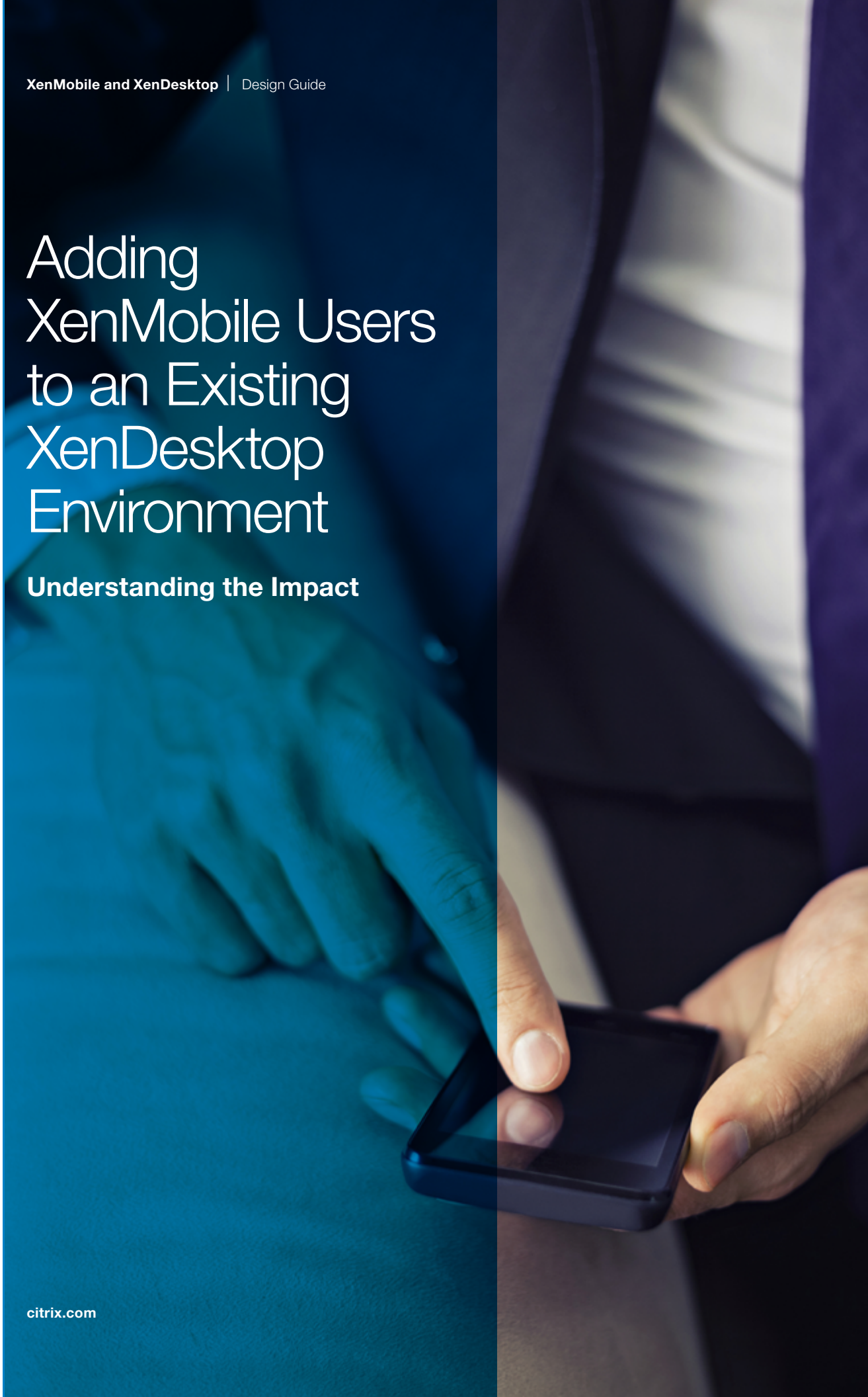
Adding XenMobile Users to an Existing XenDesktop Environment

Understanding the Impact



citrix.com

Table of Contents

Project Overview

As Citrix continues to empower people to work and collaborate from anywhere with Citrix XenDesktop and the FlexCast model, the growth of BYOD adds mobile users to the mix. Citrix XenMobile supports the mobility user across many different devices, from smartphones to tablets.

One of the common questions to ask when adding mobile users to an existing XenDesktop environment is "What is the impact to the existing environment and where are the points of intersection between XenDesktop and XenMobile users?"

For example, a company of 30,000 employees may have only 5,000 users considered remote users, but every employee may be a potential mobile user. Not all employees will be both mobile users and remote users simultaneously, but there is the potential for overlap. When deployed, XenMobile uses its own set of components to connect a mobile user who is separate from XenDesktop.

This document focuses on the intersection point between XenMobile users (mobile users) and XenDesktop users (remote users), where a NetScaler appliance provides the primary point of intersection for the two types of user. For mobile users, the main concern is Micro VPN traffic; for remote users it is ICA traffic.

Objectives

The objective of this document is to provide design guidance to ensure successful deployments by examining the impact adding mobile users have on NetScaler scalability in an existing XenDesktop environment. The aim is to understand when the remote user experience begins to be affected by the addition of mobile users, and the NetScaler appliance approaches saturation.

Assumptions

The following assumptions played a role in defining the overall strategy:

- A XenDesktop 7.x environment already exists with remote users accessing resources through a Citrix NetScaler appliance(s).
- Mobile users are being added to the existing environment.
- The XenDesktop environment has been configured to support 5,000 remote users. Login VSI will be used to generate a workload for these users.
- A tool developed by the Citrix XenMobile team will be used to generate the mobile user traffic that creates multiple micro-VPN connections per user.

Conceptual Architecture and Testing Methodology

The following diagram provides details about the conceptual architecture.

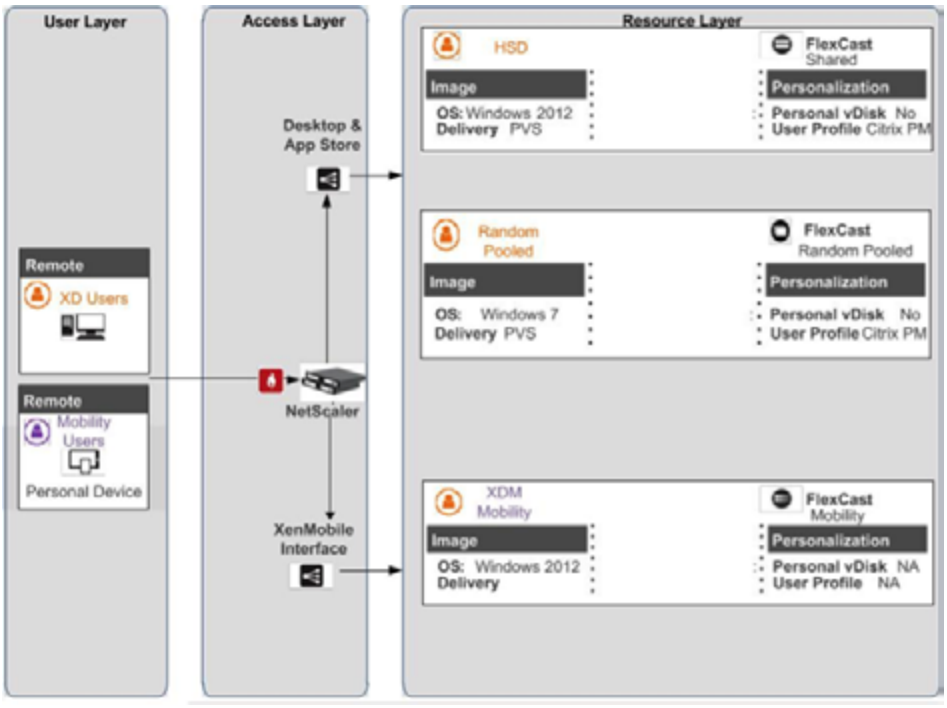


Figure 1: Conceptual Architecture

For testing, the test bed used to create the Scaling XenDesktop 7 to 5,000 users with VMware vSphere 5.1 Validated Design Guide was utilized. This ensured the 5,000 remote user count could be achieved without concern around the XenDesktop configuration.

All XenDesktop users were configured as remote users and LoginVSI 3.7 was used to drive the XenDesktop workload. The backend XenDesktop components, StoreFront, Delivery Controller, and Provisioning Services, were configured to support the 5,000 remote user workload, using the hardware and configuration described in the Validated Design Guide. StoreFront and the App Controller were not integrated.

For the mobile users, an internal Citrix test tool that completes a connection through the NetScaler appliance to an echo server in the datacenter was utilized. This tool uses the echo server to create two MicroVPN connections between the mobile users and the datacenter, simulating the two MicroVPNs created through the NetScaler appliance when a mobile user logs in and is connected. A user mix of 50/50 of IOS and Andriod users was configured.

To begin the tests, LoginVSI was started to drive the workload for the 5,000 remote users. After all 5,000 users were logged in and running sessions successfully, a 30-minute quiet period was maintained to ensure stability. After the 30-minute quiet period the Citrix XenMobile test tool was started. The tool used three load generators, each talking to a dedicated App Controller echo server on the back-end. Each load generator was configured to create 5,000 mobile users and the load generators were

started at 10-minute intervals. Each load generator simulated 833 mobile users logging on per hour and staying logged on for the remainder of the test. With all three load generators running at once, the logon load was 2499 mobile users per hour. Previous testing had shown that simulating higher logon numbers than that caused failures on the back-end echo server, as it was unable to keep up. It should be noted that in XenMobile, App Controllers can be configured into cluster and failover appliance modes to create a scalable redundant configuration. In this test environment, however, one launcher was configured to a single App Controller in the data center to provide better control on managing the launch process.

To monitor the testing environment, NetScaler Insight was used. NetScaler Insight uses AppFlow, (AppFlow.org) an open standards technology that includes per-flow level application and networking data. NetScaler Insight Center was set up as the central point for collecting ICA traffic and used for monitoring and analyzing ICA performance. Command Center was used for monitoring and analyzing the performance of the NetScaler MPX 10500 appliance for CPU and memory. The NetScaler appliance was configured in transparent mode, meaning that ICA traffic was not transmitted over a VPN. NetScaler Insight was also configured in transparent mode and an Appflow policy was set to collect all ICA traffic.

The NetScaler appliance was configured to support both remote and mobile users. Configuration information is defined in Appendix B. Certificate authorization was not configured.

Test Results

One of the data points collected by NetScaler Insight is the ICA session Round Trip Time (RTT) for users. During the "quiet" period this value, along with NetScaler CPU utilization and memory were monitored to develop a baseline for the 5,000 users. The following chart shows a snapshot of the 5,000 user ICA RTT prior to staring the test clients.

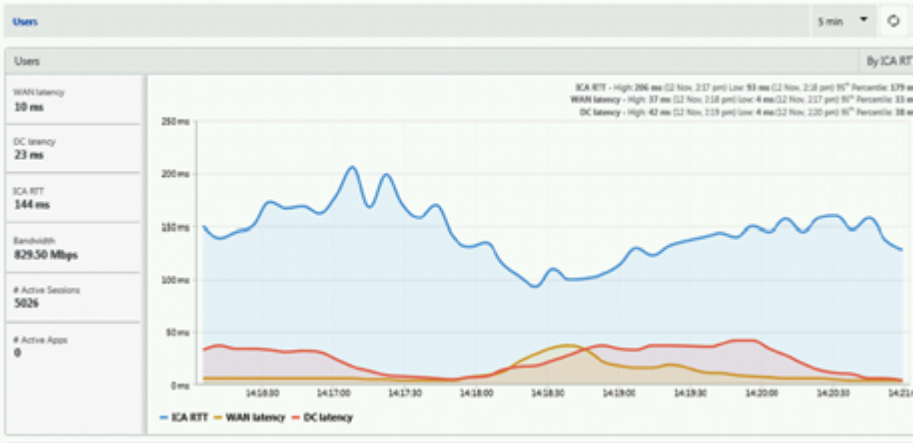


Figure 2: 5,000 users ICA RTT Base

The ICA RTT at this point was averaging 144ms and this number was used as the baseline. After the "quiet" period was complete, the Citrix XenMobile test tool was started. The following chart shows the CPU utilization from the start of the test. Note that there is a one hour time diffverence between the ICA RTT chart and the CPU utilization chart.

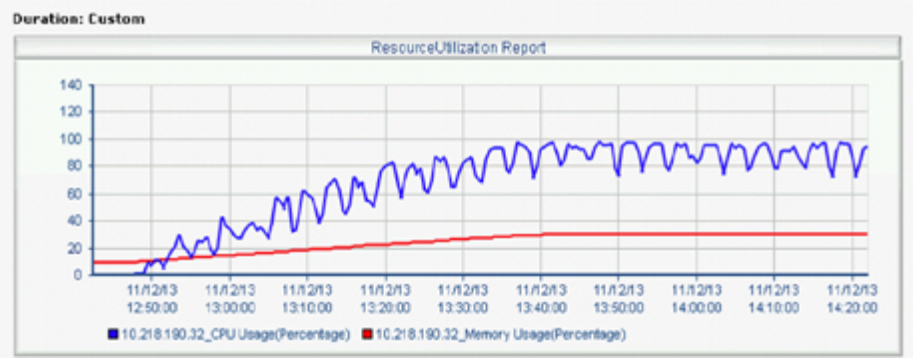


Figure 3: CPU Utilization

At 13:20, the CPU Utilization chart aligned with the ICA RTT chart, showing the 5,000 remote users were consuming an average of 60% of the NetScaler appliance CPU and approximately 20% of the NetScaler appliance memory.

As the mobility workload increased, CPU utilization approached 100% while memory utilization levelled out at 30%. The following table shows the different mobile user workloads and impacts.

# Mobile Users	Dropped	ICA RTT	CPU %	Memory %
0 (Baseline)		144	50	20
833		120	65	25
1666		102	80	30
2499		120	80	30
3332		155	80	30
4165		166	85	30
5831		166	85	30
6664		128	85	30
7497		128	85	30
8330	3	189	85	30
9163	4	123	85	30
9996	1	151	85	30
10829		146	90	30
11662	1	155	95	30
12495	1	119	95	30
13328	14	191	95	30

Table 1: ICA RTT/CPU Utilizations

The CPU values are estimated averages for when the ICA RTT snapshot was taken. No NetScaler best practices were applied to spread the load, which would have affected CPU utilization. Investigation has shown that about 15% of CPU utilization was caused by AppFlow policies that were monitoring and managing the NetScaler appliance.

Looking at the table, an anomaly occurs at 3332 users, with a 23% jump in ICA RTT times. No remote users were dropped, however, and the remote user experience was not affected. At 8330 mobile users, there was a 32% jump in ICA RTT times and remote users started to be dropped.

The dropped users show the first major inflection point and put the number of mobile users within the 7,500 range with 5,000 remote users.

Scaling

The next step in testing was to determine if there was scaling as the number of remote users changed. Using the same test bed configuration, tests were executed at 3,000 and 4,000 remote users to determine if a trend could be found. The following chart shows CPU and memory utilization for the 3,000-user test run baseline and at the start of the testing.

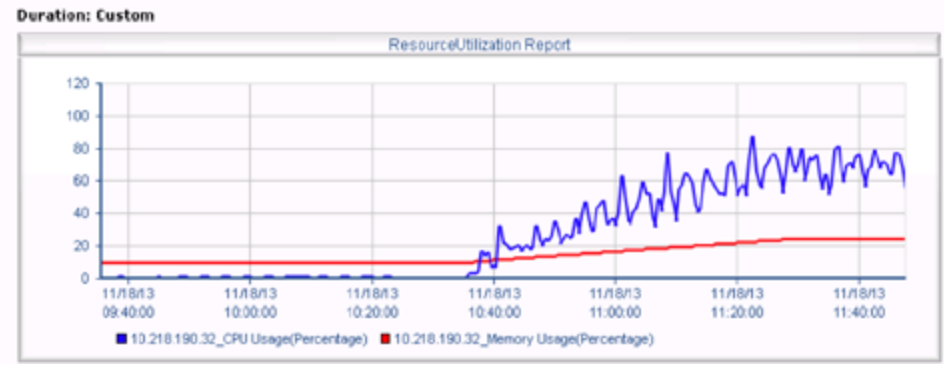


Figure 4: CPU/Memory Utilization (3,000 Remote Users)

The baseline ICA RTT was taken at 10:40 and was 36ms. At this point, CPU utilization was just over 20%, and memory utilization was around 10%. As the number of mobile users increased to 14,000, CPU utilization approached 85%, as seen in the chart below:

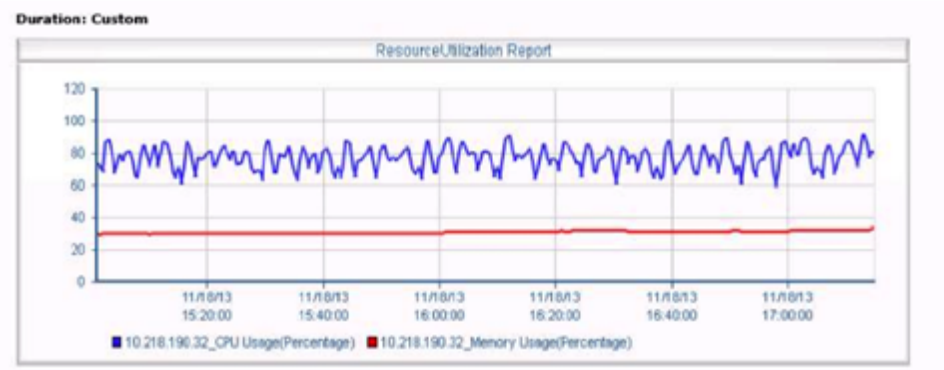


Figure 5: CPU/Memory Utilization (3,000 Remote Users) as Mobile User numbers increase

As the number of mobile users increased, passing 14,000, the response times from the NetScaler appliance to both NetScaler Insight Center and Command Center increased. Investigation of the logs after the test completed showed that with 14,000 mobile users the ICA RTT times remained in the 35-45ms range, however the NetScaler appliance had reached capacity.

When increasing to 4,000 remote users the baseline ICA RTT times jumped to the mid-50ms range, as an average and CPU utilization was slight higher, closer to 35-40%, before mobile users started logging on.

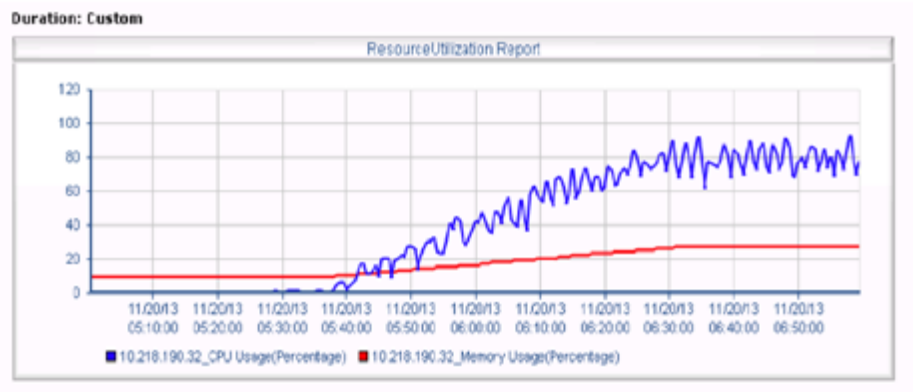


Figure 6: CPU/Memory Utilization (4,000 Remote Users)

CPU utilization across the baseline showed good linear scaling going from 3,000 to 5,000 users. For 4,000 users, CPU utilization became very steady at about 85% with around 11,000 to 12,000 mobile users logged on, as shown in the following chart.

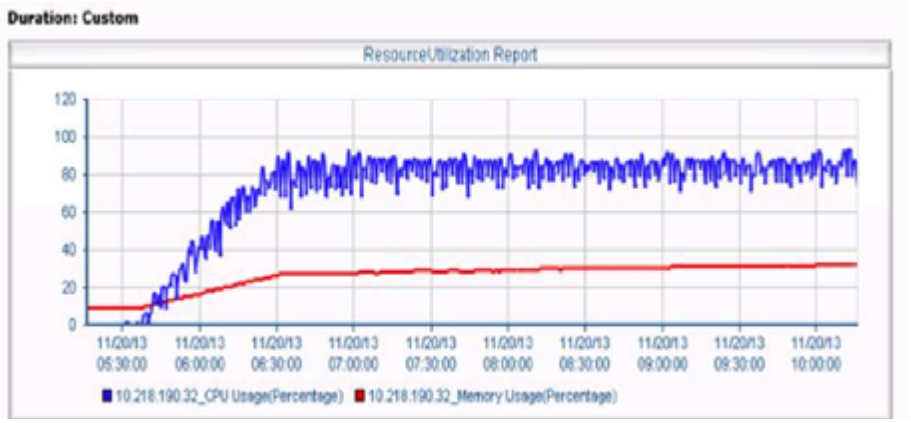


Figure 7: CPU/Memory Utilization (4,000 Remote Users) as Mobile User numbers increase

CPU utilization was very steady at 80% for most of the run, but connection time started to increase over 14,000 mobile users and the CPU utilization average moved closer to over 90%.

In all cases, memory utilization increased to approximately 30-35% and held steady.

Conclusions

The following table provides information about the recommend number of mobile users:

Remote users	Mobile Users	MicroVPN Connections
50/50 IOS/Andriod		
5,000	7,500	15,000
4,000	11,000	22,000
3,000	14,000	28,000

For a mobile user, a successful connection creates two MicroVPN connections through the NetScaler appliance. It should also be noted that each XenMobile application, for example, WorxMail or WorxWeb, also creates multiple MicroVPN connections. The Citrix XenMobile test tool created two MicroVPN connections, per user connecting, and these MicroVPNs were maintained for the entire test run. Converting the number of mobile users to MicroVPN connections, for the 5,000-user test, means close to 15,000 MicroVPN connections. Mobile users must be considered in terms of MicroVPNs since each XenMobile application creates a MicroVPN. The recommended numbers are not at 100% CPU utilization, but are focused at an 85% average, without dropping any remote users. In the 5,000 user test, remote users started dropping at the 8330 mobile user load. The scaling trend shows that decreasing the number of remote users by 1000 increases the number of mobile users by approximately 3,000, or 6,000 MicroVPN connections.

Extrapolating out the numbers, if zero remote users then the MPX 10500 appliance would support approximately 23,000 mobile users (46,000 mVPN connections) at 90% utilization of the NetScaler appliance. This is very much in line with testing done by the Citrix XenMobile group utilizing a similarly configured MPX 10500 NetScaler.

Summary

In summary, the goal of this document was to provide an understanding of the impact mobile users have on existing remote users at the intersection point, the NetScaler appliance.

NetScaler Insight Center was used to monitor the NetScaler appliance during testing and worked very well, but as noted, it can affect the performance of the NetScaler appliance depending on how the tool is configured.

Remote access and networking is a very complex environment with many different areas to tune and adjust. For this testing, the defaults were used and no tuning was performed. Any changes or tuning that may affect CPU utilization will almost certainly affect mobile users. The goal of this testing was to examine the impact of adding mobile users to an existing XenDesktop environment and to evaluate NetScaler performance.

All testing was done on a NetScaler MPX 10500 appliance with 8 CPU cores and a 2.8 MHz processing speed. Newer NetScaler appliances will provide improved performance and increased numbers, but the scaling numbers will be helpful in determining starting points for configuring mobile users into an existing XenDesktop environment.

Appendix A: Configuring Appflow for transparent-mode data collection

This appendix provides details about the commands to run to configure transparent mode data collection manually on the NetScaler MPX 10500 appliance.

Note: You cannot configure transparent mode in NetScaler Insight Center.

At the command prompt, do the following:

1. SSH into the NetScaler appliance.
2. Specify the ICA ports on which the NetScaler appliance listens for ICA traffic, as follows:

```
set ns param -icaPorts 2598 1494
```

```
> show appflow param
        AppFlow parameters

        IPFIX template refresh interval: 3600 seconds
        Appname refresh interval: 600 seconds
        IPFIX flow record export interval: 60 seconds
        IPFIX UDP Path MTU: 1472 bytes
        HTTP URL logging: ENABLED
        AAA username logging: ENABLED
        HTTP cookie logging: ENABLED
        HTTP referer logging: ENABLED
        HTTP method logging: ENABLED
        HTTP host logging: ENABLED
        HTTP user-agent logging: ENABLED
        HTTP Content-Type header logging: DISABLED
        HTTP Authorization header logging: DISABLED
        HTTP Via header logging: DISABLED
        HTTP X-Forwarded-For header logging: DISABLED
        HTTP Location header logging: DISABLED
        HTTP Setcookie header logging: DISABLED
        HTTP Setcookie2 header logging: DISABLED
        Log only client-side traffic: NO
        Connection Chaining: DISABLED
 Done
```

3. Add NetScaler Insight Center as an AppFlow collector on the NetScaler appliance, as follows:

```
add appflow collector <name> -IPAddress <ip_addr>
```

```
> show appflow collector
1)      Name: af_collector_192.168.153.30
        IPv4 address: 192.168.153.30
        UDP port: 4739
        Netprofile:
 Done
>
```

4. Create an AppFlow action and associate the collector with that action, as follows:

add appflow action <name> -collectors <string> …

```
> show appflow action

1)      Name: af_action_192.168.153.30
        Collectors: af_collector_192.168.153.30
        Hits: 11990
        Action Reference Count: 1
Done
```

add appflow policy pol true act

```
> show appflow policy
1)      Name: af_policy_sfagee.hp1xd7esx.com_192.168.153.30
        Hits: 11990
        Undef Hits: 0
        Active: Yes
```

5. Bind the appflow policy to a global bind point, as follows:

bind appflow global <policyname> <priority> -type <type>

```
> bind appflow global af_policy_sfagee.hp1xd7esx.com_192.168.153.30 1 -type ICA_REQ_DEFAULT
Done
>
```

bind appflow global pol 1 -type ICA_REQ_DEFAULT
Note: The value for type should be ICA_REQ_OVERRIDE or ICA_REQ_DEFAULT to apply to ICA traffic.

```
> show appflow global
1)      Global bindpoint: ICA_REQ_DEFAULT
        Number of bound policies: 1

Done
>
```

6. Set the value of the flowRecordInterval parameter for AppFlow to 60 seconds, as follows:

set appflow param -flowRecordInterval 60

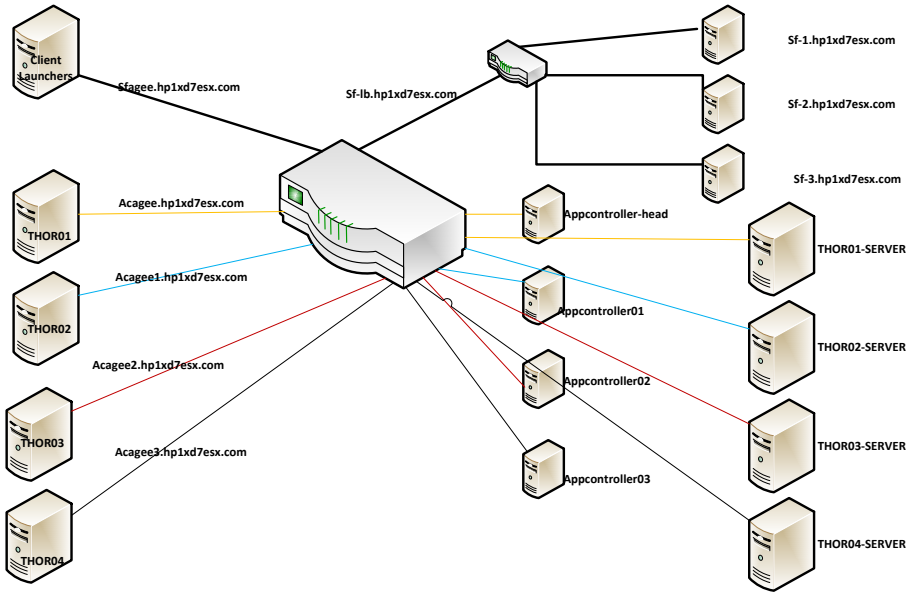
7. Save the configuration, as follows:

save ns config

Appendix B: NetScaler Configuration

Current NetScaler Configuration

Platform	NSMPX-10500 8*CPU+2*E1K+16*E1K+8*CVM 1620 760000
CPU	2835MHZ
Software	NetScaler NS10.1: Build 120.1316.e.nc, Date: Oct 30 2013, 09:23:13
Network connections	Three Physical (Management Link, LAN Link, and WAN Link)



VPN vServer Configuration

NetScaler was configured with five VPN vServers:

- **Sfagee.hp1xd7esx.com**. Used for ICA sessions. Sessions that came in on this vServer were redirected to a LB VIP (separate virtual NetScaler) which ultimately load balanced the traffic to one of three StoreFront servers.
- **Acagee.hp1xd7esx.com**, Acagee1.hp1xd7esx.com, Acagee2.hp1xd7esx.com, and Acagee3.hp1xd7esx.com. Used for mobile users. Each redirected to a specific App Controller for SSO and application enumeration.

Corporate Headquarters
Fort Lauderdale, FL, USA

India Development Center
Bangalore, India

Latin America Headquarters
Coral Gables, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

Online Division Headquarters
Santa Barbara, CA, USA

UK Development Center
Chalfont, United Kingdom

EMEA Headquarters
Schaffhausen, Switzerland

Pacific Headquarters
Hong Kong, China

About Citrix
Citrix (NASDAQ:CTXS) is a leader in virtualization, networking and cloud infrastructure to enable new ways for people to work better. Citrix solutions help IT and service providers to build, manage and secure, virtual and mobile workspaces that seamlessly deliver apps, desktops, data and services to anyone, on any device, over any network or cloud. This year Citrix is celebrating 25 years of innovation, making IT simpler and people more productive with mobile workstyles. With annual revenue in 2013 of $2.9 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million people globally. Learn more at www.citrix.com.

0314/PDF **citrix.com**