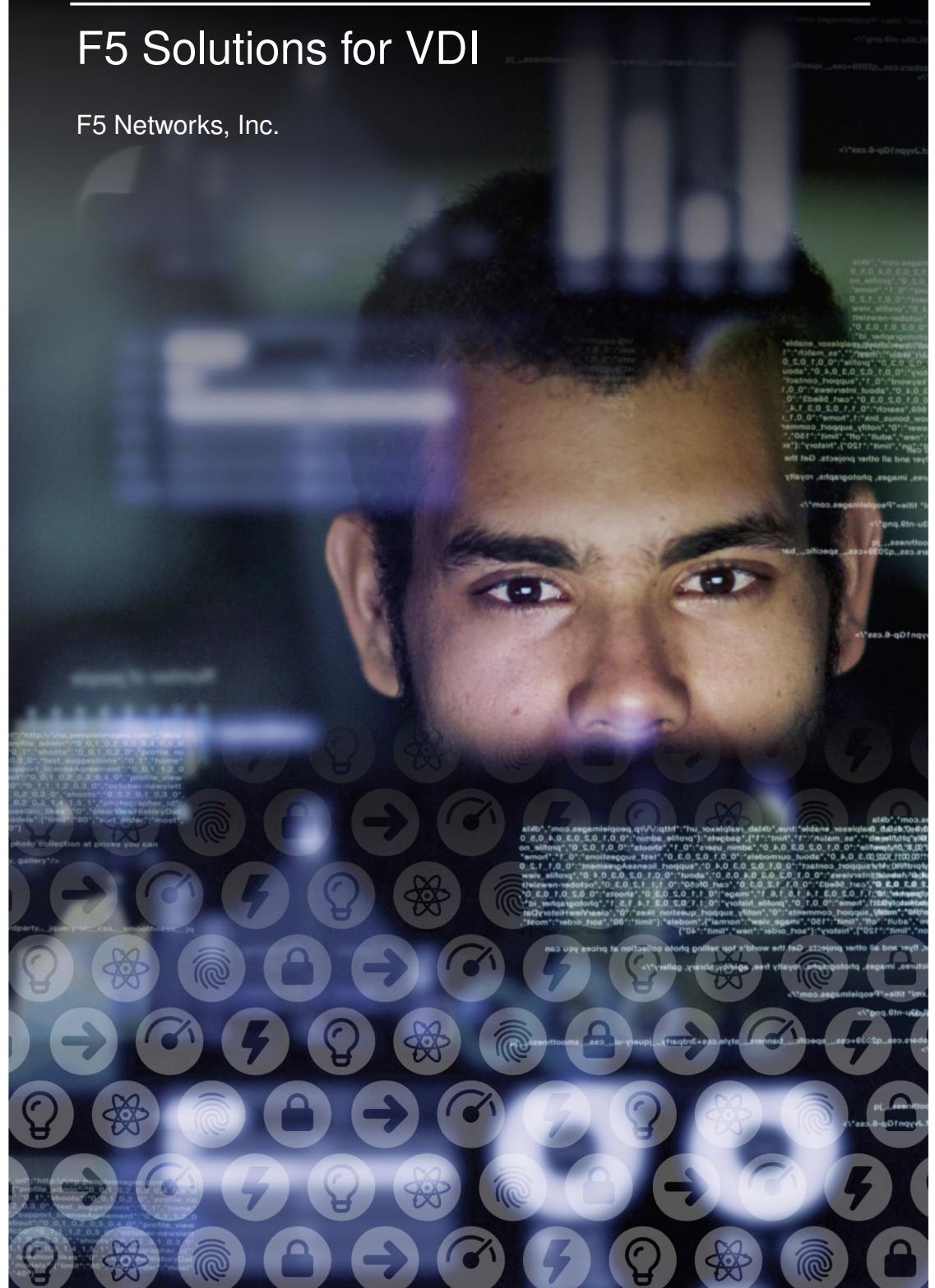




Agility 2017 Hands-on Lab Guide

F5 Solutions for VDI

F5 Networks, Inc.



Contents:

1	201: VDI the F5 Way	5
1.1	Getting Started	5
1.2	Module 1: Solutions for VMware View	7
1.3	Module 2: Solutions for Citrix XenDesktop	18
1.4	Module 3: Microsoft RDS Proxy	22

1

201: VDI the F5 Way

Welcome to “VDI the F5 Way” lab. This guide is intended to complement lecture material provided by “VDI the F5 Way” course. The purpose of this lab is to demonstrate how F5 technologies can integrate with industry leading virtual desktop infrastructure (VDI). In general, we will take you through the process of current deployment to a simplified and more secure topology with F5 BIG-IP.

1.1 Getting Started

Please follow the instructions provided by the instructor to start your lab and access your jump host.

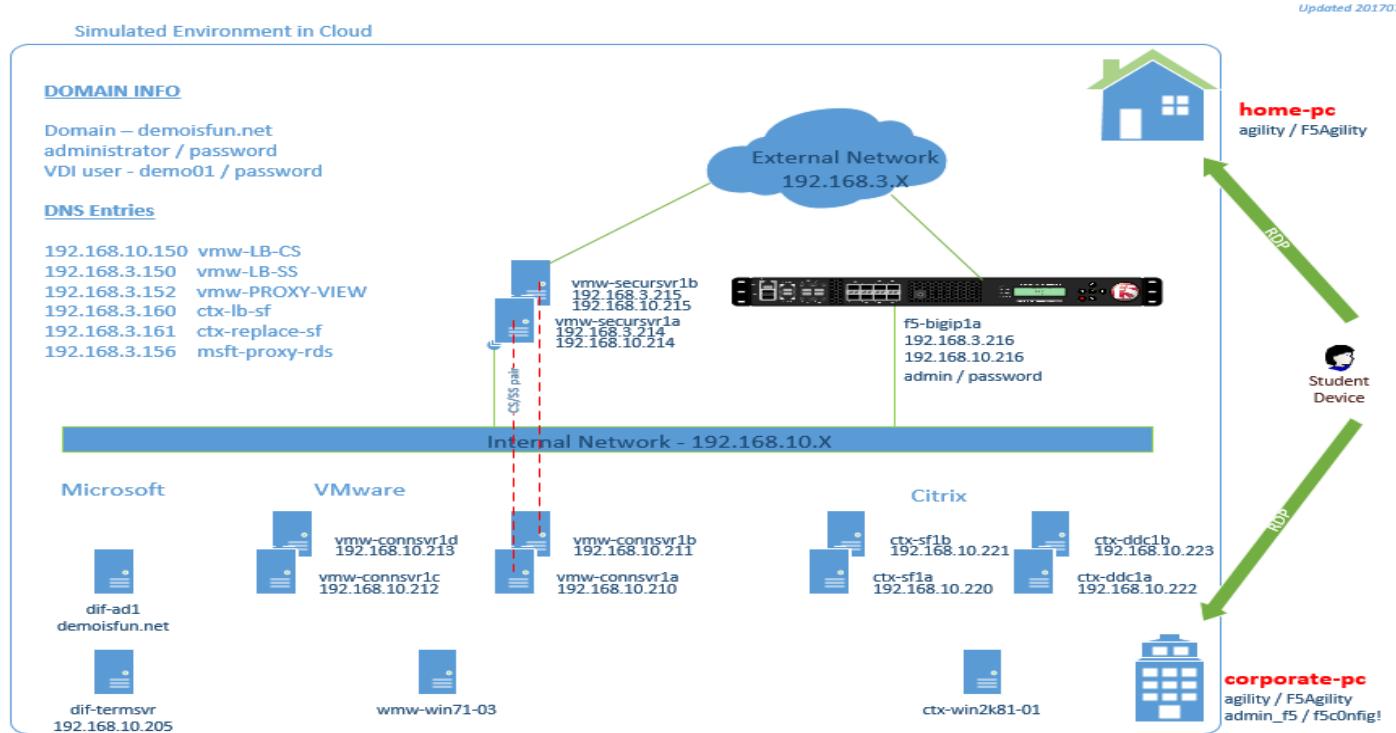
Note: All work for this lab will be performed exclusively from the Windows jumphost. No installation or interaction with your local system is required.

1.1.1 Lab Network Setup

In the interest of focusing as much time as possible on this solution, we have provided some resources and basic setup ahead of time. These are:

- The system has been licensed and provisioned for LTM and APM
- A Microsoft Active Directory environment has been configured for authentication
- A working VMware Horizon View environment has already been configured
- A working Citrix XenDesktop environment has already been configured
- Windows desktops with Citrix and View clients will be accessed using RDP to demonstrate functionality

AGILITY Lab - VDI the F5 way

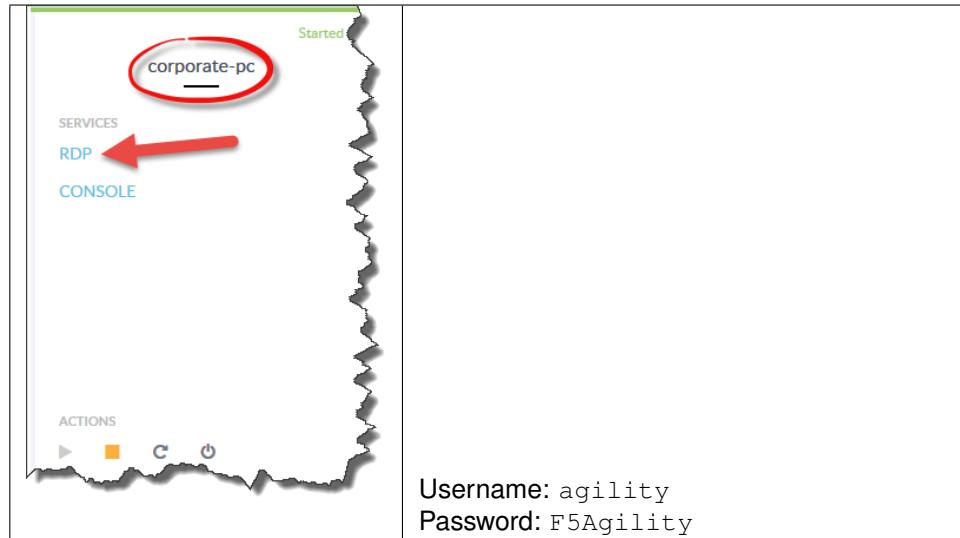


1.1.2 Connect to Lab Environment

Please refer to Figure 1. We are simulating internal and external access to VDI with 2 Windows desktops. When viewing the “corporate-pc” session, imagine you are sitting at your office desk. Likewise, viewing the “home-pc” session is like you are sitting at home, or anywhere outside of the company network.

The lab is hosted in a cloud provider Ravello. Lab instructors will provide a URL and a unique student number to access the environment. Each attendee is expected to have a computer with a modern browser and a RDP client.

1. Open browser and go to the URL provided by instructor.
2. Scroll down and find “corporate-pc”. Choose to connect with RDP. Leave this connection for entire lab duration.



1. Scroll down and find “home-pc”. Choose to connect with RDP. Leave this connection for entire lab duration.



1.2 Module 1: Solutions for VMware View

The purpose of this lab is to build out 3 basic VMware View architectures leveraging F5 load balancing and authentication functionality.

- Construct VMware View implementations with F5 LTM and APM software modules
- Familiarize student with F5 iApp templates

Estimated completion time: 60 Minutes

1.2.1 Lab 1.1: Solutions for VMware View

Task 1 – Access VMware View Desktop environment without F5

Test the functional VMware view environment using the internal Connection Servers (Internal use case without F5 integration)

Access the VDI with a client on the internal network. The workstation will be preconfigured to initiate the connection through a specific connection server. Security servers are not used by internal VDI users

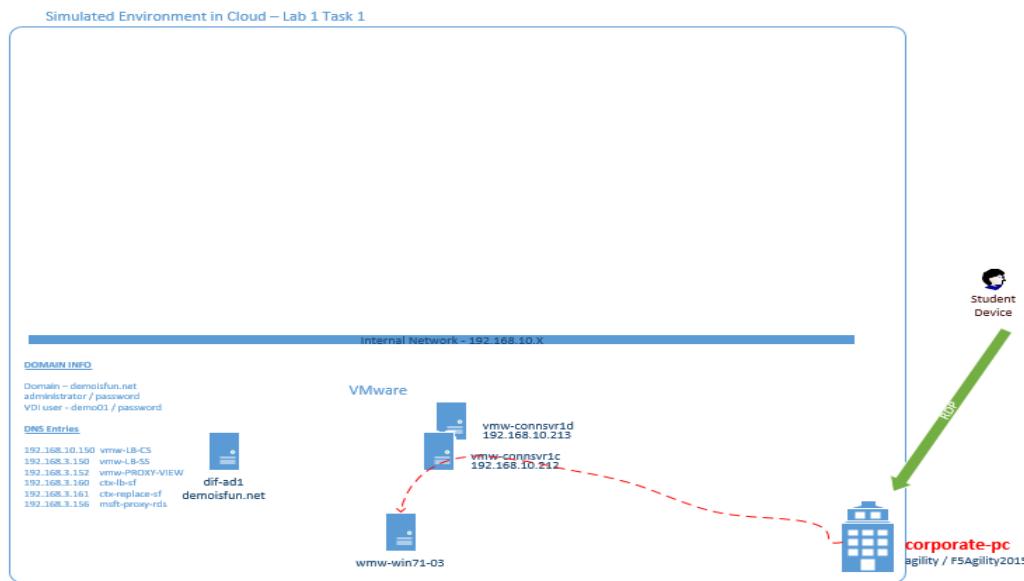
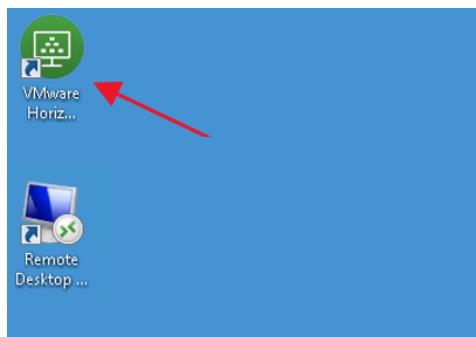


Figure 2 - Accessing Internal View Desktop

1. From the “corporate-pc”.
2. Use the VMware Horizon View client to access the connection server



- VMware Horizon Client
 - + New server
3. Connection Server address “vmw-connsrv1c.demoisfun.net”
 4. When prompted for credentials
 - Username: demo01
 - Password: password
 5. Double-click the “Agility” icon to launch virtual desktop.

6. In the Agility virtual desktop, open Notepad and type in something.
7. Disconnect from Agility desktop by closing View client. (RDP Toolbar on top. May need to slide the blue RDP bar to the left in order to click the X in Agility Toolbar)
8. Open View client and try to reconnect to “vmw-connsrv1c. demoisfun.net”
9. Notepad should still be on the desktop with the text you input.
10. Close the View client. (press the X in Agility Toolbar)
11. Keep the RDP session open for Task 2

Task 2 – Load Balance Connection Servers

Use the F5 iApp for VMware View to configure a load balancing environment for the Connection Servers. This will increase the number of Connection Servers available to internal users and load balance access to these resources (Internal use case with F5 load balancing)

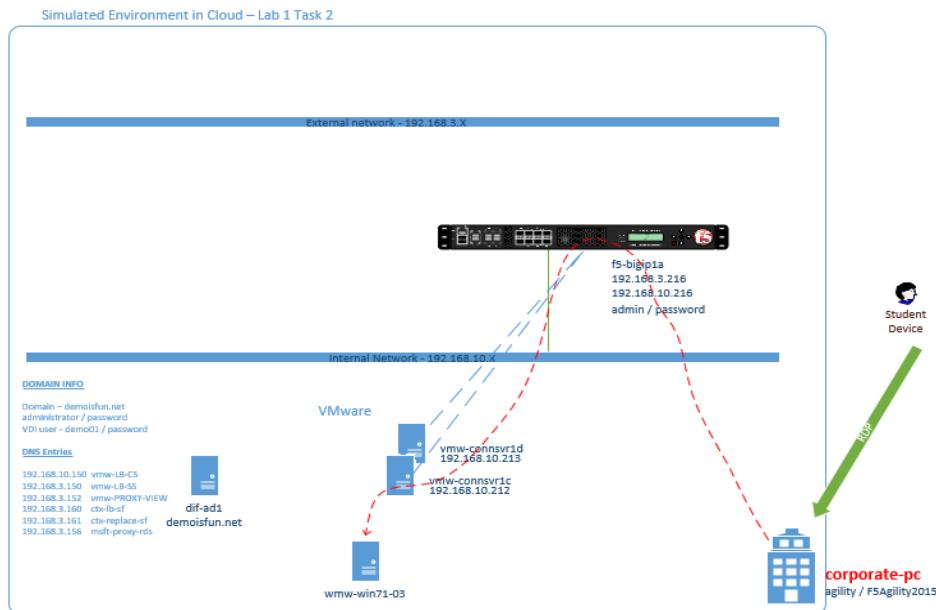


Figure 3 - Load balance Connection Servers

Deploy the iApp

1. From “corporate-pc”.
2. Use browser to access the F5 Admin GUI
 - <https://f5-bigip1a.demoisfun.net>
 - Username: admin
 - Password: password
3. Create a new Application Service
 - iApps >> Application Services
 - Press the **Create** button
 - Name the Application Service **VM_LAB_1_LBCS**
 - Select **f5.vmware_view.v1.5.1** for the template

4. Review the **Welcome to the iAPP template for VMware Horizon View**
5. Note the **Template Options** (leave these default)
6. **Big-IP Access Policy Manager** (Set this to **No** for this exercise)
7. **SSL Encryption** (Certs are preloaded for this exercise)

How should the BIG-IP system handle encrypted traffic?	Terminate SSL for clients, re-encrypt to View servers (SSL-bridging)
Which SSL certificate do you want to use?	wild.demoisfun.net.crt
Which SSL private key do you want to use	wild.demoisfun.net.key

8. **PC Over IP** (leave these default – No PCoIP connections...)
9. **Virtual Servers and Pools**

What virtual server IP address do you want to use for remote, untrusted clients?	192.168.10.150
What is the associated service port?	443
What FQDN will clients use to access the View environment	vmw-LB-CS.demoisfun.net
Which Servers should be included in this pool	192.168.10.212 192.168.10.213

10. **Client Optimization** (leave these default—Do not compress...)
11. **Application Health**
 - Use the pulldown to select a standard https monitor
12. Press the **Finished** button

View the objects which were created by the iApp

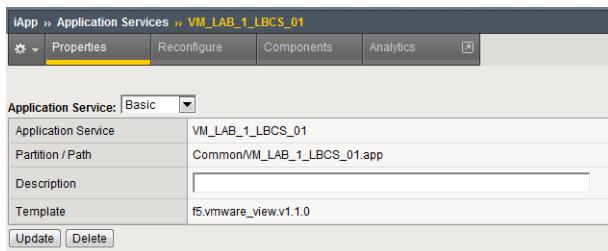
1. Select the Components tab at the top of the page

Name	Availability	Type
VM_LAB_1_LBCS_01	Offline	Application Service
VM_LAB_1_LBCS_01_https	Offline	Virtual Server
VM_LAB_1_LBCS_01_pool_0	Offline	Pool
http		Monitor

2. Is the Virtual server available?
3. Are the pool members available?
4. What is the node status? Why?
5. Note that a persistence profile was created
 - Check Match Across Services
 - Press update
 - Note the error at the top of the page
6. Return to iApp>>Application Services
7. Review the remaining parameters (any questions)

View the properties of the iApp

1. Select the Properties tab at the top of the page



2. Use the pull down next to Application Service:
3. Select Advanced
4. Note the check in Strict Updates
 - Is this related to the screen when editing the persistence profile?
 - What are the pro's and con's of unchecking this parameter?

Test the connection server load balancing using both VMware View client and browser access methods.

1. From "corporate-pc"
2. Open View client and connect to the Virtual Server just created with iApp.
 - + New Server
 - vmw-LB-CS.demoisfun.net
 - Connect Button
 - * IP address will not work—Certificate contains demoisfun.net
 - 3. When prompted for credentials
 - Username: demo01
 - Password: password
 - Login Button
 - 4. Double-click Agility icon to launch View desktop
 - 5. Verify that the Agility desktop functions
 - 6. Close the View client. (May need to slide the RDP Toolbar out of the way)
 - 7. Open IE and browse to <https://vmw-LB-CS.demoisfun.net>
 - 8. Select VMware Horizon View HTML access
 - 9. Log in
 - Username: demo01
 - Password: password
 - 10. Double click to launch Agility desktop
 - 11. At the Cert Warning, click "Continue to this website"

12. Verify that the Agility desktop functions
13. Close the IE browser window

Task 3 – Access View Desktop through Security Server

Test the functional VMware View environment using external Security Servers. (External use case without F5 integration)

This environment shows a user connecting to a native VMware security server which is statically mapped to a VMware connection server. This is a non-redundant external access model

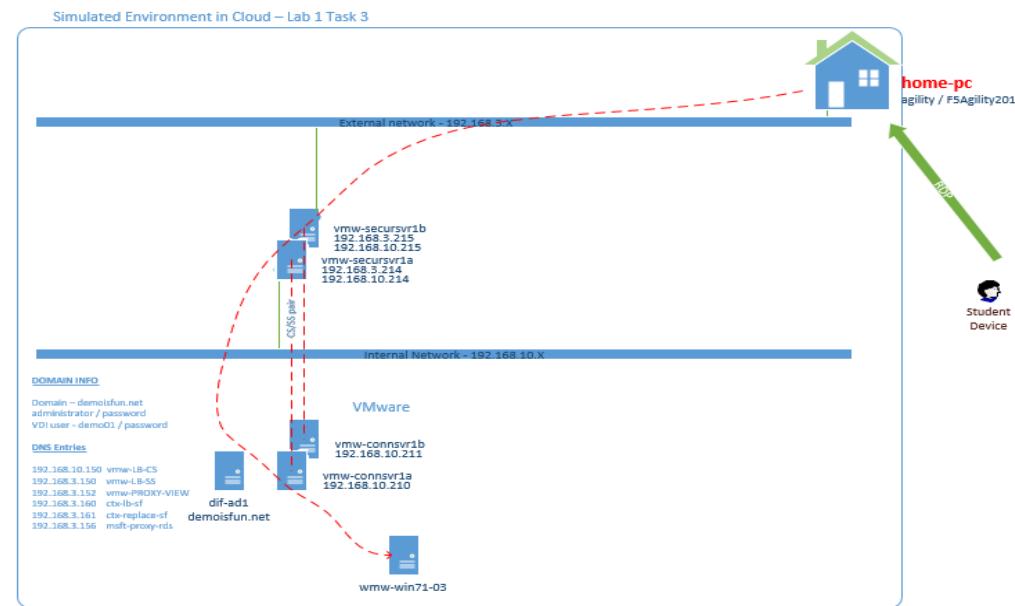


Figure 4 - Access external View Desktop

1. From the “home-pc”



2. Use the VMware Horizon View client to access the security server
 - + New Server
 - Security Server address `vmw-secursvr1a.demoisfun.net`
 - Press Connect Button
3. When prompted for credentials

- Username: demo01
 - Password: password
4. Double-click Agility icon to launch desktop
 5. Close the View client
 6. Access the application through your browser <https://vmw-secursvrla.demoisfun.net>
 7. Select VMware Horizon View HTML access
 - Username: demo01
 - Password: password
 8. Double-click Agility icon to launch desktop
 9. Accept Cert at warning
 10. Select (Agility)
 11. Verify that the desktop functions
 12. Close the browser window

Task 4 – Load Balance Security Servers

Use the F5 iApp for VMware View to configure a load balancing environment for the Security Servers. This will increase the number of Security Servers available to internal users and load balance access to these resources (External use case with F5 load balancing)

This environment load balances 2 external facing Security Servers. These Security Servers are directly mapped to 2 existing connection servers in the environment (not the 2 Connection Servers that are load balanced in the steps above)

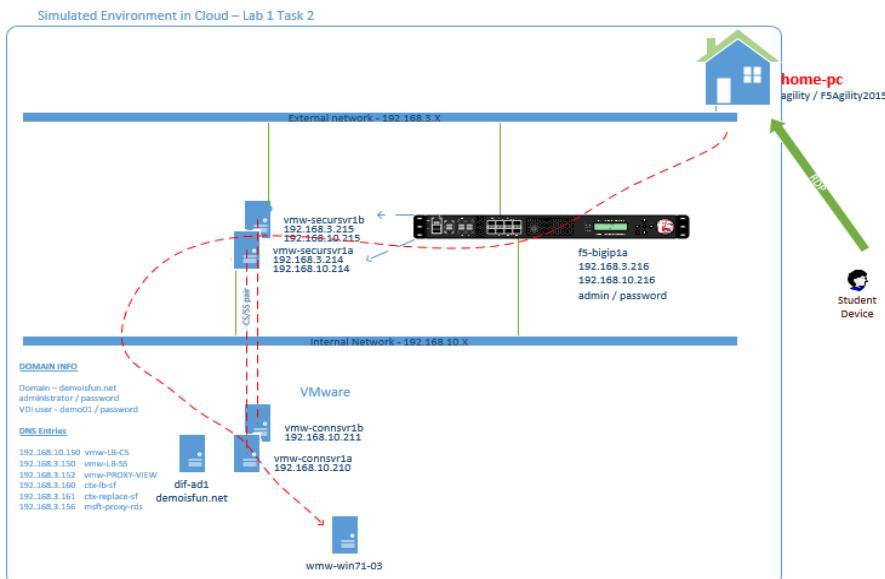


Figure 5 - Load balance Security Servers

Deploy the iApp

1. From “corporate-pc”

2. Create a new Application Service by selecting
 - iApps >> Application Services
 - Press the **Create** button
 - Name the Application Service VM_LAB_1_LBSS
 - Select f5.vmware_view.v1.5.1 for the template
3. Review the **Welcome to the iAPP template for VMware Horizon View**
4. Note the **Template Options** (leave these default)
5. **Big-IP Access Policy Manager** (Set this to **No** for this exercise)
6. **SSL Encryption** (Certs are preloaded for this exercise)

How should the BIG-IP system handle encrypted traffic?	Terminate SSL for clients, re-encrypt... (SSL-Bridging)
Which SSL certificate do you want to use?	wild.demoisfun.net.crt
Which SSL private key do you want to use?	wild.demoisfun.net.key

7. **PC Over IP** (leave these default – No PCoIP connections...)
8. **Virtual Servers and Pools**

What virtual server IP address do you want to use for remote, untrusted clients?	192.168.3.150
What FQDN will clients use to access the View environment?	vmw-LB-SS.demoisfun.net
Which Servers should be included in this pool?	192.168.3.214 192.168.3.215

9. **Application Health**
 - Use the pulldown to select a standard https monitor
10. Press the **Finished** button

View the objects which were created by the iApp

1. Select the Components tab at the top of the page
2. Is the Virtual server available?
3. Are the pool members available?
4. Is the Node Available?
5. Review the remaining parameters (any questions)

Test the Security Server load balancing using both VMware View client and browser access methods

1. From “home-pc”
2. Open View client and connect to the Virtual Server just created with iApp.
 - + New Server

- vmw-LB-SS.demoisfun.net (192.168.3.150)
 - Press the Connect button
 - IP address will not work—Certificate contains demoisfun.net
3. When prompted for credentials
 - Username: demo01
 - Password: password
 4. Double-click Agility icon to launch desktop
 5. Verify the desktop functions
 6. Close the View client
 7. Open IE and browser to
 - <https://vmw-LB-SS.demoisfun.net>
 8. Select VMware Horizon View HTML access
 9. Enter Credentials
 - Username: demo01
 - Password: password
 10. Select (Agility)
 11. Accept Cert warning
 12. Select (Agility)
 13. Verify that the desktop functions
 14. Close the browser window

Task 5 – Replace Security Servers and leverage APM as a PCOIP proxy

This environment will utilize Big-IP as a PCOIP Proxy. This eliminates the requirement for all Security Servers. The Connection Servers will be load balanced. Authentication is handled by the F5 APM module

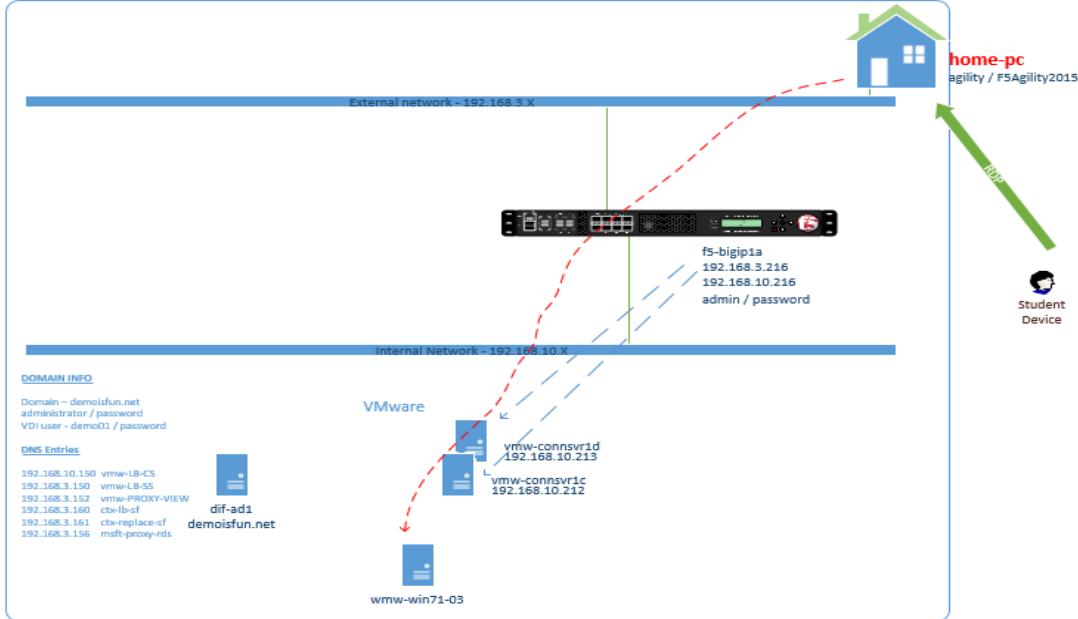


Figure 6 - Replace Security Servers

Deploy the iApp

1. From “corporate-pc”
2. Create a new Application Service by selecting iApps -> Application Services and selecting Create
 - iApps >> Application Services
 - Press the **Create** button
 - Name the Application Service VM_LAB_1_PCOIP
 - Select f5.vmware_view.v1.5.1 for the template

iApp Configuration

1. Review the **Welcome to the iAPP template for VMware Horizon View**
2. Note the **Template Options** (leave these default)
3. **BIG-IP Access Policy Manager**

Do you want to deploy BIG-IP Access Policy Manager?	Yes, deploy BIG-IP Access Policy Manager
Do you want to support browser based connections, including the View HTML5 client?	Yes, support HTML 5 view clientless browser connections
Should the BIG-IP system support RSA SecureID two-factor authentication	NO, do not support RSA SecureID two-factor authentication
Should the BIG_IP system show a message to View users during logon	No, do not add a message during logon
What is the NetBIOS domain name for your environment	demoisfun
Create a new AAA Server object or select an existing one	AD1

4. SSL Encryption (Certs are preloaded for this exercise)

How should the BIG-IP system handle encrypted traffic?	Terminate SSL for clients, re-encrypt... (SSL-Bridging)
Which SSL certificate do you want to use?	wild.demoisfun.net.crt
Which SSL private key do you want to use?	wild.demoisfun.net.key

5. PC Over IP (leave these default)

6. Virtual Servers and Pools

What virtual server IP address do you want to use for remote, untrusted clients?	192.168.3.152
What FQDN will clients use to access the View environment?	vmw-PROXY-VIEW.demoisfun.net
Which Servers should be included in this pool?	192.168.10.212 192.168.10.213

7. Application Health

- Use the pull down to select a standard https monitor
8. Press the **Finished** button

View the objects which were created by the iApp

1. Select the Components tab at the top of the page
2. Note the increase in objects compared to Task 2 and Task 4
3. Are the pool members available?
4. Note the APM objects which were not present in the prior exercises
5. Review the remaining parameters (any questions)

Test the APM (PCoIP) functionality using both VMware View client and browser access methods

1. From "home-pc"
2. Open IE and browse to <https://vmw-PROXY-VIEW.demoisfun.net>
 - Username: demo01
 - Password: password
3. Click Agility on APM webtop
4. Select VMware View Client
5. Note the error and inspect the certificate
6. Close the error box and cert view boxes
7. Close the View client
8. Open IE and browse to
 - <https://vmw-PROXY-VIEW.demoisfun.net>

9. Select VMware Horizon View HTML access

10. Enter Credentials

- Username: demo01
- Password: password

11. Click Agility

12. Select HTML5 Client

13. Verify that the desktop functions

14. Close the browser

1.3 Module 2: Solutions for Citrix XenDesktop

The purpose of this module is to build out 2 common F5 deployment with XenDesktop.

Note: The connectivity in this environment is slower than a typical production environment—please be patient

1.3.1 Lab 2.1: Solutions for Citrix XenDesktop

Task 1 – Access XenDesktop without F5

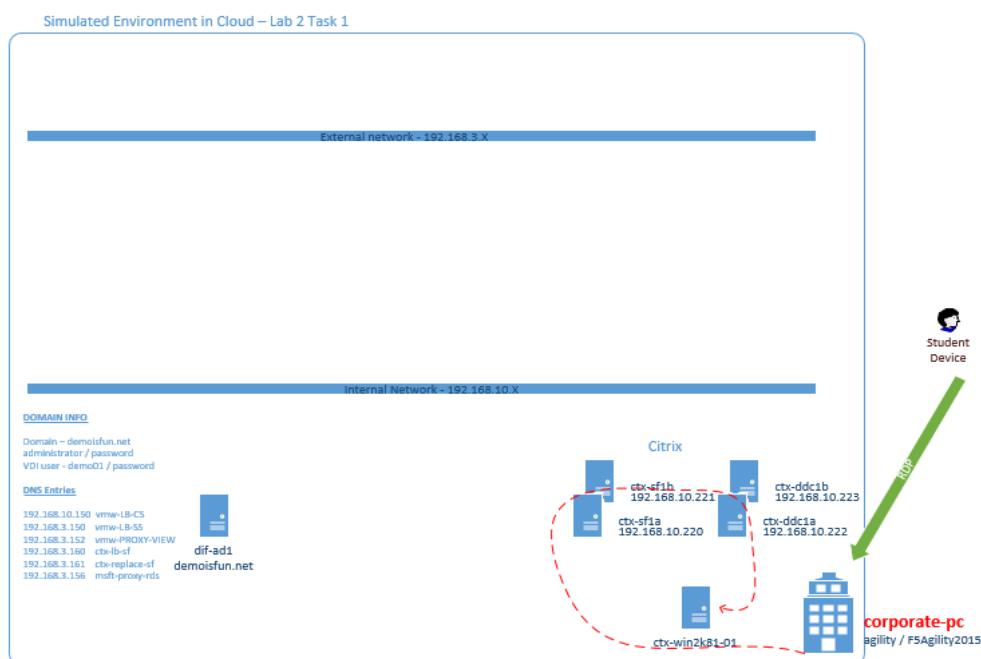


Figure 7 - Access XenDesktop through StoreFront

1. From “corporate-pc”
2. Use IE and browse to Citrix Storefront
 - <http://ctx-sf1a.demoisfun.net/Citrix/AgilityStoreWeb/>

3. When prompted for credentials
 - Username: demoisfun\demo01
 - Password: password
4. Click “Agility” to launch XenDesktop.

Note: This takes a long time due to the Ravello implementation*

5. Citrix “Desktop Viewer” launches and connects to XenDesktop
6. Verify virtual desktop function
7. In Citrix Agility desktop, click Start and Logoff
8. Log off the Citrix receiver client using the 01 Demo pulldown in the upper right corner
9. Close the browser Window

Task 2 – Load Balance StoreFront

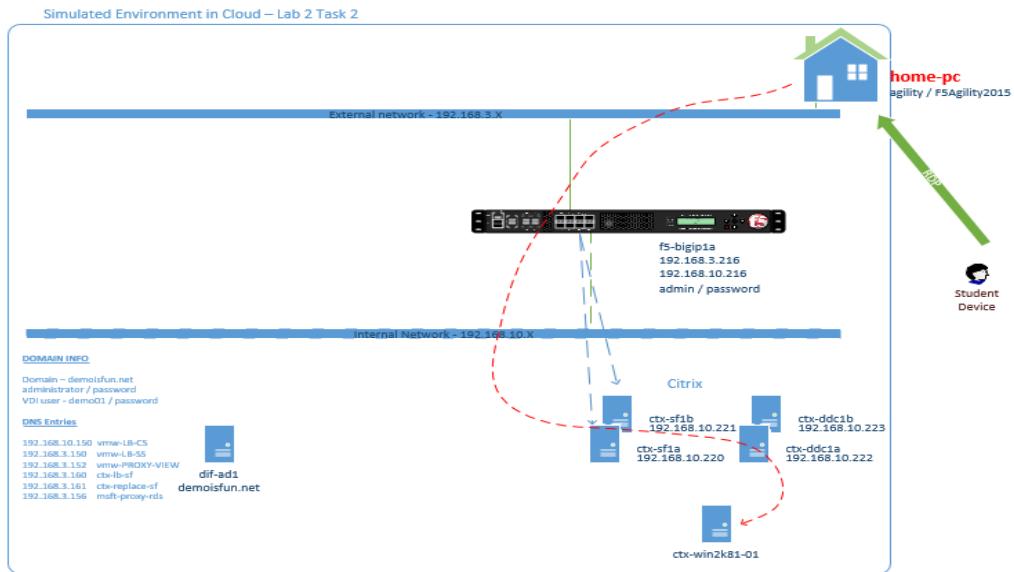


Figure 8 - Load balance StoreFront

Deploy the iApp

1. From “corporate-pc”
2. Create a new Application Service by selecting iApps -> Application Services and selecting Create
 - iApps >> Application Services
 - Press the **Create** button
 - Name the Application Service VM_LAB_2_LBSF
 - Select f5.citrix_vdi.v2.4.1rc1 for the template

iApp Configuration

1. Review the **Welcome to the iApp template for XenDesktop and XenApp**

2. **General**

Use APM to securely proxy application (ICA) traffic and authenticate users into your Citrix environment?	Yes, Proxy ICA traffic and authenticate users with BIG_IP
What is the Active Directory NetBIOS Domain Name used for your Citrix servers?	demoisfun

3. **BIG-IP Access Policy Manager**

Do you want to replace Citrix Web Interface or StoreFront servers with the BIG-IP system?	"No, do not replace..."
Create a new AAA object or select an existing one?	AD1

4. **Virtual Server for Web Interface or StoreFront servers**

How should the BIG-IP system handle encrypted traffic to Web Interface or StoreFront servers?	Terminate SSL for Clients, Plaintext to Citrix servers (SSL offload)
Which SSL certificate do you want to use?	wild.demoisfun.net.crt
Which SSL private key do you want to use?	wild.demoisfun.net.key
What IP address will clients use to access the Web Interface or StoreFront servers, or the F5 Webtop?	192.168.3.160
Did you deploy Citrix StoreFront?	Yes, ... StoreFront 3.0 or 3.6 Note: we are running SF 3.9
What is the URI used on StoreFront or Web Interface servers for XenApp or XenDesktop?	/Citrix/AgilityStoreWeb/ <i>Note that this is the same URL used to access citrix directly in Task 1</i>

5. **Web Interface or StoreFront servers**

What DNS name will clients use to reach the Web Interface or StoreFront servers?	ctx-LB-SF.demoisfun.net
Which port have you configured for Web Interface or StoreFront HTTP traffic?	80
What are the IP addresses of your Web Interface or StoreFront servers?	192.168.10.220 192.168.10.221
Which Monitor do you want to use	http

6. **Virtual Server for XML Broker or Desktop Delivery Controller (DDC) Servers**

What IP address do you want to use for the XML Broker or DDC farm virtual server?	192.168.10.161
How will requests from the Web Interface or StoreFront servers arrive?	XML Broker or DCC requests will arrive unencrypted (HTTP)

7. **XML Broker or DDC Servers**

What are the IP addresses of your XML Broker or DDC servers?	192.168.10.222 192.168.10.223
Which monitor do you want to use?	http

8. Press the **Finished** button

Test connectivity

1. Use the RDP function on your laptop to connect to the “home-pc”
2. Launch IE and browse to,
 - <http://ctx-lb-sf.demoisfun.net>
3. When prompted for credentials
 - Username: demo01
 - Password: password
4. Storefront is displayed with Agility icon
 - Click “Agility” to launch XenDesktop
5. In the Citrix Agility desktop, click Start and Logoff
6. Log off the Citrix receiver client using the 01 Demo pulldown in the upper right corner
7. Close the browser Window

Task 3 – Replace StoreFront

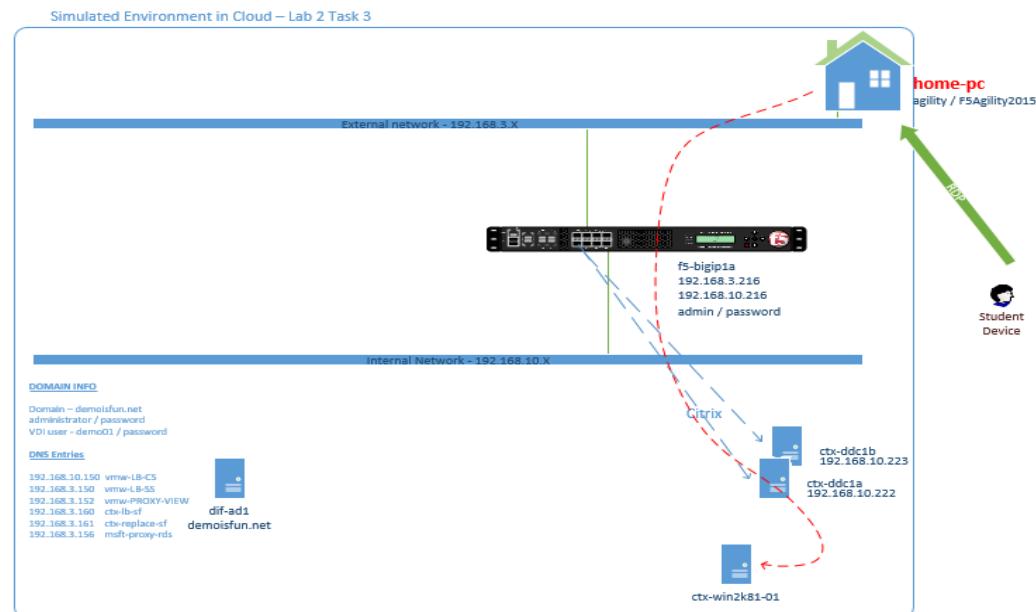


Figure 9 - BIG-IP replaces StoreFront

Deploy the iApp

1. From “corporate-pc”

2. Create a new Application Service by selecting iApps -> Application Services and selecting Create
 - iApps >> Application Services
 - Click on VM_LAB_2_LBSF
 - Click the **Reconfigure** link near the top

iApp Configuration

1. **BIG-IP Access Policy Manager**

Do you want to replace Citrix Web Interface or StoreFront servers with the BIG-IP system?	"Yes, replace Citrix..."
---	--------------------------

2. Scroll through the template and note that the storefront pool members are no longer present
3. Press the **Finished** button

Test connectivity

1. From "home-pc"
2. Launch IE and browse to
 - <http://ctx-lb-sf.demoisfun.net>
3. When prompted for credentials
 - Username: demo01
 - Password: password
4. APM webtop is displayed with Agility icon
5. Click on Agility to launch XenDesktop
6. Click Open to launch the Citrix ICA client (*pop up box at bottom*)
7. Verify that desktop is functional
8. In Citrix Agility desktop, click on Start and Logoff
9. Logout of APM Webtop using the Logout button in the upper right corner
10. Close the browser window

1.4 Module 3: Microsoft RDS Proxy

The purpose of this module is access an internal RDS server from an external client.

1.4.1 Lab 3.1: Microsoft RDS proxy

The purpose of this lab is access an internal RDS server from an external client.

Task 1 – Access Terminal Server from external network

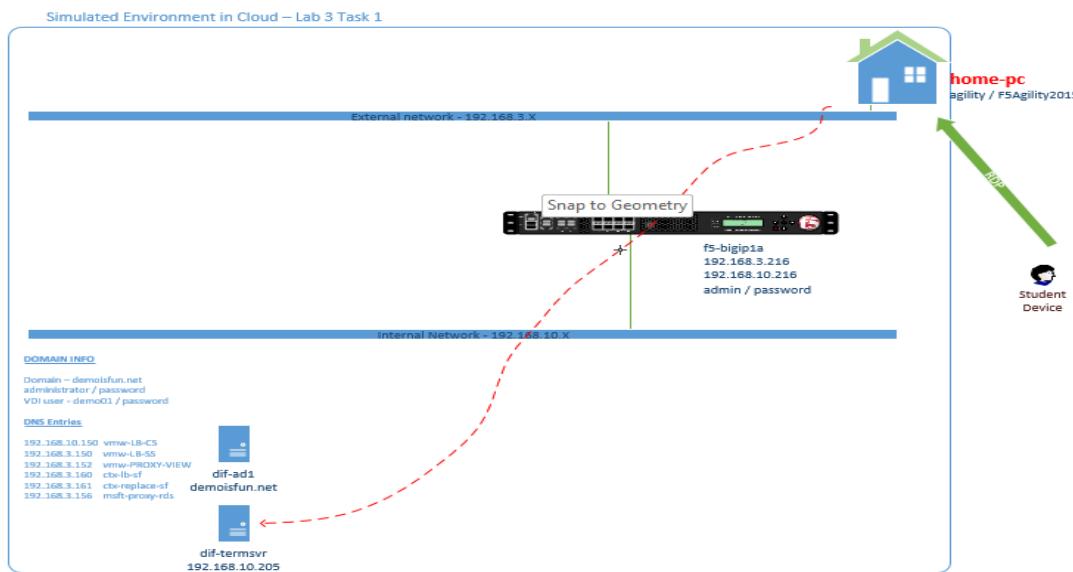


Figure 10 - BIG-IP proxy RDP connection

Deploy the iApp

1. From “corporate-pc”
2. Connect to the F5 config GUI
 - <https://f5-bigip1a.demosifun.net>
 - Username: admin
 - Password: password
3. Create an NTLM Machine Account
 - Access >>Authentication>>NTLM>>Machine Account

Name	AD1-f5-bigip1a
Machine Account Name	f5-bigip1a
Domain FQDN	demosifun.net
Domain Controller FQDN	dif-ad1.demosifun.net
Admin User	administrator
Password	password

4. Click the **JOIN** button to create the machine account
5. Create a new Application Service by selecting iApps -> Application Services and selecting Create
 - iApps >> Application Services
 - Press the **Create** button
 - Name the Application Service VM_LAB_3_RDS
 - **Select f5.microsoft_rds_remote_access.v1.0.2 for the template**

iApp Configuration

1. Review the **Welcome to the iApp template for Remote Desktop Gateway**

2. Template Options

Do you want to deploy BIG-IP APM as an RDP proxy?	Yes, deploy BIG-IP Access Policy Manager
---	--

3. Access Policy Manager

Do you want to create a new AAA server, or use an existing AAA server?	AD1
Which NTLM machine account should be used for Kerberos delegation?	AD1-f5-bigip1a

4. SSL Encryption

Which SSL certificate do you want to use?	wild.demoisfun.net.crt
Which SSL private key do you want to use?	wild.demoisfun.net.key

5. Virtual Servers and Pools

What IP address do you want to use for the virtual server(s)?	192.168.3.156
How would you like to secure your hosts?	Allow any host

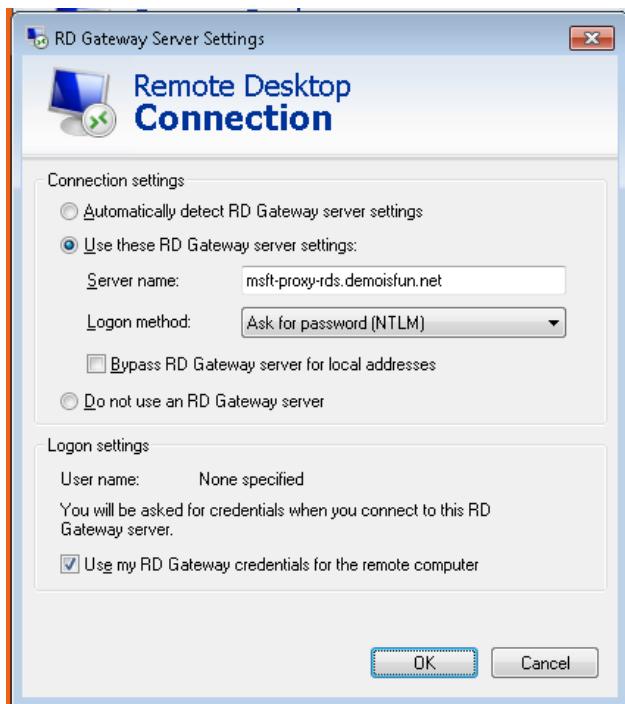
6. Press the **Finished** button

Test the RDS proxy functionality using RDS Client

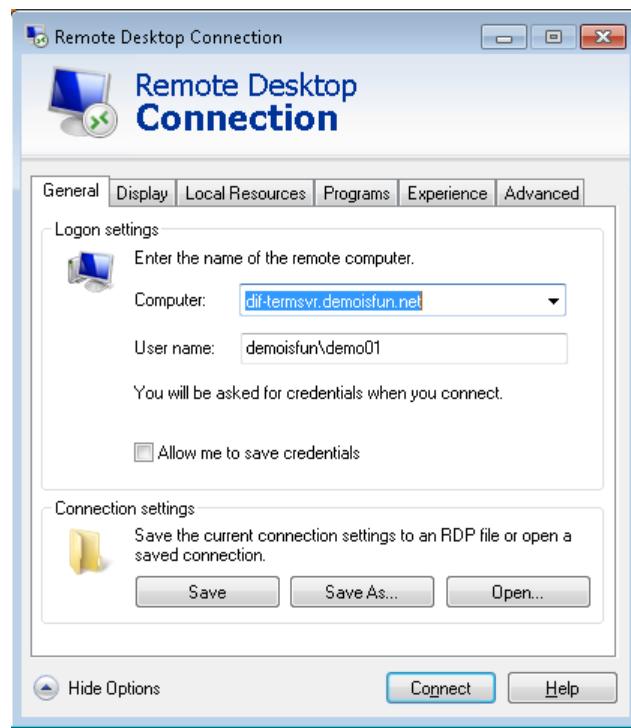
1. From “home-pc”

2. Launch RDS client (on desktop).

- Select the “Show Options” Pulldown
- Select the “Advanced” tab
- Click the Settings button
- In the “RDS Gateway...” window,
 - In Server name field, type in msft-proxy-rds.demoisfun.net. Note this address resolves to the address 192.168.3.156 which was configured in the iApp



- Verify the other default settings on this window
 - Click OK
3. Under “General” tab, in the “Computer” field, type in the name of the host you want to RDP to which is dif-termsvr.demoisfun.net
- In the “User name” field, type in demoisfun\demo01



- Click “Save”

- Click “Connect”
4. When prompted for credentials
- Username: demo01
 - Password: password
5. Accept Certificate warning



6. You are connected to dif-termsvr.demoisfun.net
7. From “corporate-pc”, open IE to Connect to BIG-IP GUI at
- <https://f5-bigipla.demoisfun.net>
8. On the left side menu, click Access -> Overview -> Active Sessions
9. Click on the session to view details

10. Log off using the windows start icon in the lower left corner

FINAL GRADE

...for this “VDI the F5 Way” lab team. Please complete the **SURVEY** to let us know how we did. We value your feedbacks and continuously looking for ways to improve.

THANK YOU FOR CHOOSING F5 !!!

WE MAKE APPS



FASTER.
SMARTER.
SAFER.



F5 Networks, Inc. | f5.com

US Headquarters: 401 Elliott Ave W, Seattle, WA 98119 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: fj-info@f5.com
©2017 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. These training materials and documentation are F5 Confidential Information and are subject to the F5 Networks Reseller Agreement. You may not share these training materials and documentation with any third party without the express written permission of F5.