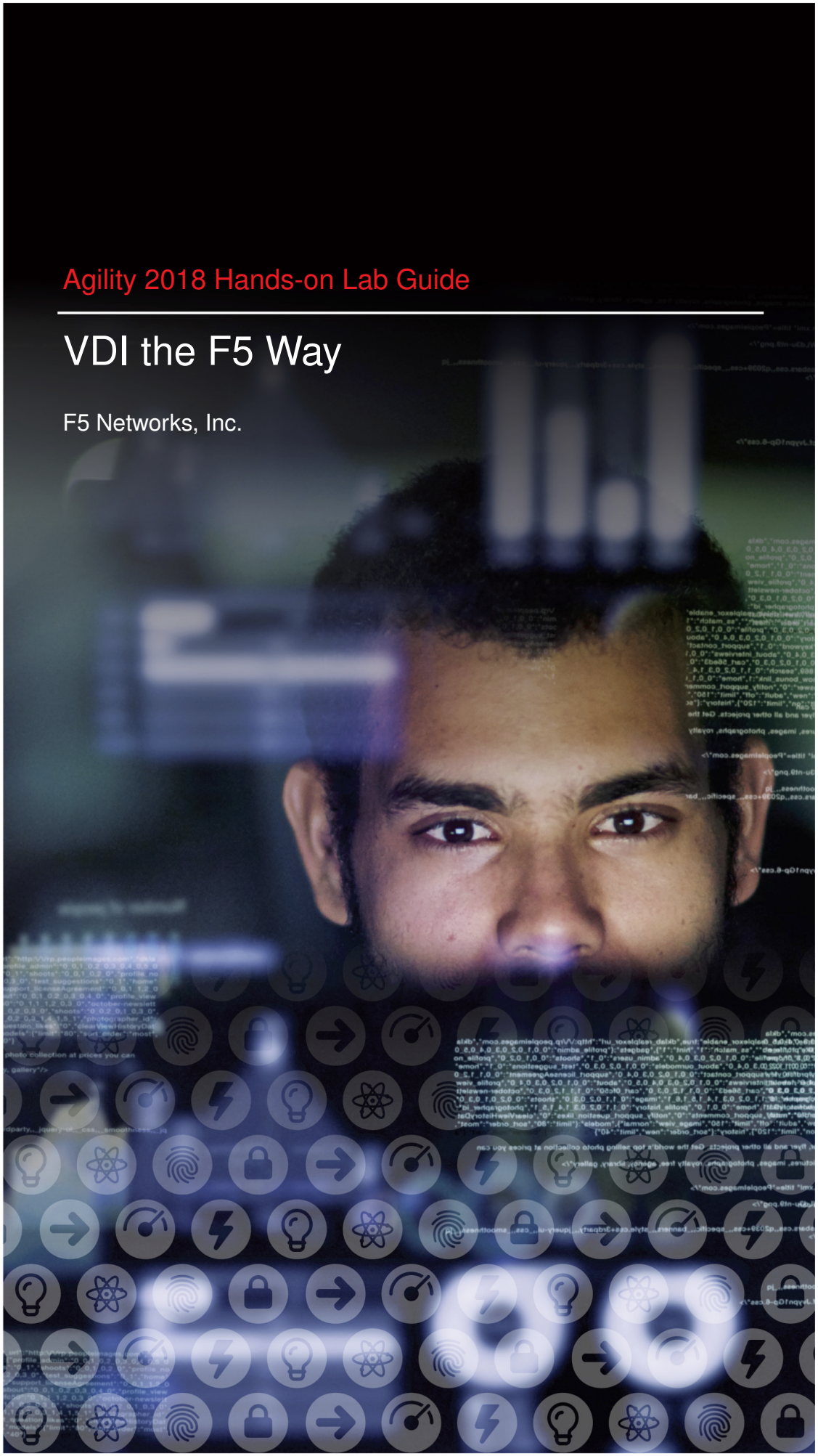


Agility 2018 Hands-on Lab Guide

VDI the F5 Way

F5 Networks, Inc.

Contents

1 Lab1 - Getting Started **5**
- 1.1 Jump Host . . . 5
- 1.2 Lab Network Setup . . . 5
- 1.3 Connect to Lab Environment . . . 7

2 Lab 2 - Solutions for VMware View **9**
- 2.1 Task 1 – Access Horizon Desktop environment without F5 . . . 9
- 2.2 Task 2 – Load Balance Connection Servers . . . 11
- 2.3 Task 3 – Access Horizon Desktop through the UAG Server . . . 14
- 2.4 Task 4 – Load Balance UAG Servers . . . 15
- 2.5 Task 5 – BIG-IP proxy View traffic in place of UAG . . . 19

3 Lab 3 - Solutions for Citrix XenDesktop **23**
- 3.1 Task 1 – Access XenDesktop without F5 . . . 23
- 3.2 Task 2 – Load Balance StoreFront . . . 23
- 3.3 Task 3 – BIG-IP Replaces StoreFront . . . 27

4 Lab 4 - Proxy for Microsoft RDS **29**
- 4.1 Task 1 – Access Terminal Server from external network . . . 29

5 Lab 5 - Consolidate VDI Access **35**
- 5.1 Task 1 – Build a VIP with an Access Policy allowing access to VMware and Citrix . . . 35

6 Final Grade **41**

1

Lab1 - Getting Started

Welcome to *"VDI the F5 Way"* lab. This guide is intended to complement lecture material provided by the *"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 Jump Host

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.

1.2 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 VMware Horizon View environment has already been configured
- A Citrix XenDesktop environment has already been configured
- A Microsoft RDS has already been configured
- Windows desktops with Citrix and View clients will be accessed using RDP to demonstrate functionality

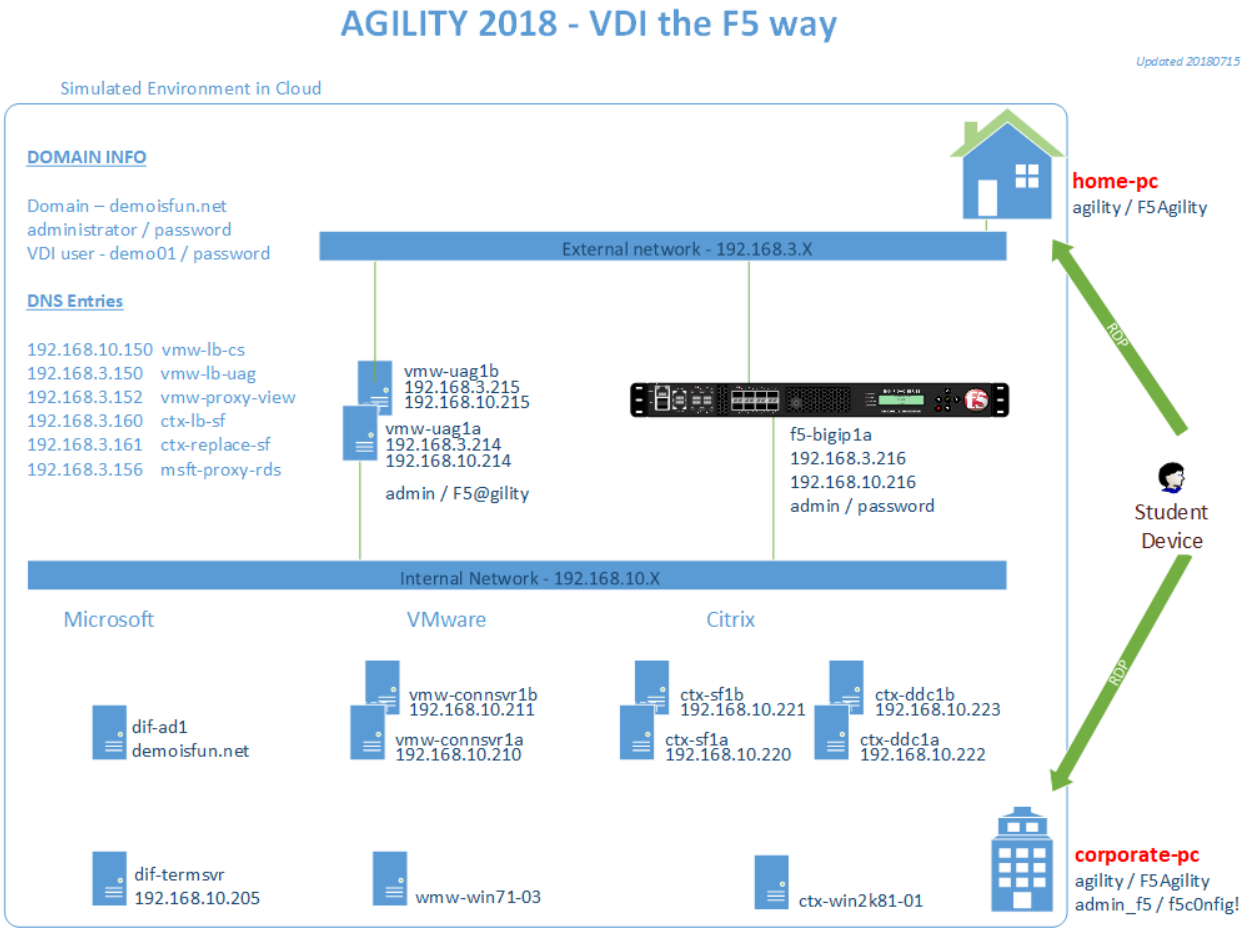


Fig. 1.1: *Complete lab setup*

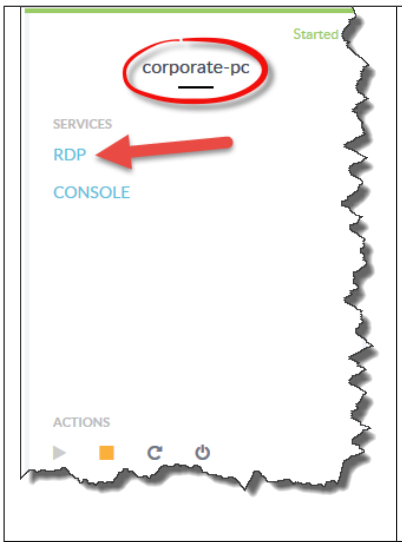
1.3 Connect to Lab Environment

Please refer to *Fig 1.1*. 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 our 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 an RDP client.

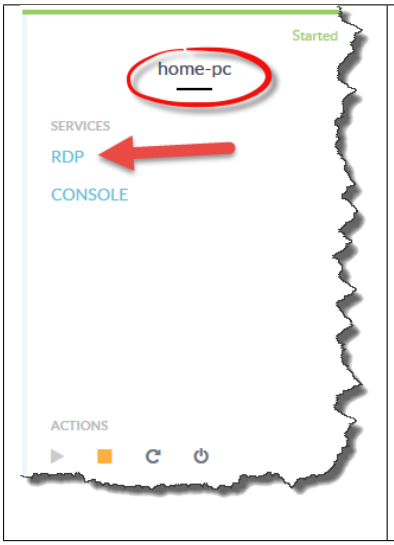
To connect to jump hosts,

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.



Username: `agility` (*Student Agility*)
Password: `F5Agility`

3. Scroll down and find *"home-pc"*. Choose to connect with RDP. Leave this connection for entire lab duration.



Username: `agility` (*Student Agility*)
Password: `F5Agility`

2

Lab 2 - 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.

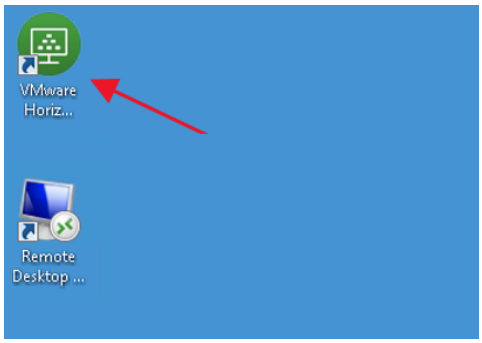
- Construct VMware View implementations with F5 LTM and APM software modules
- Familiarize student with F5 iApp templates

Estimated completion time: *60 Minutes*

2.1 Task 1 – Access Horizon Desktop environment without F5

Access the Horizon Desktop using the Horizon Client on the internal network. Horizon Client points directly to a Connection Server. This step is to verify Horizon is working and BIG-IP is not in the path. (Internal use case without F5 integration)

1. From the *"corporate-pc"*
2. On the desktop, launch the Horizon Client



3. Click **New Server**
4. Type in the Connection Server address `vmw-connsvr1a.demoisfun.net`
5. When prompted for credentials
    - Username: `demo01`
    - Password: `password`

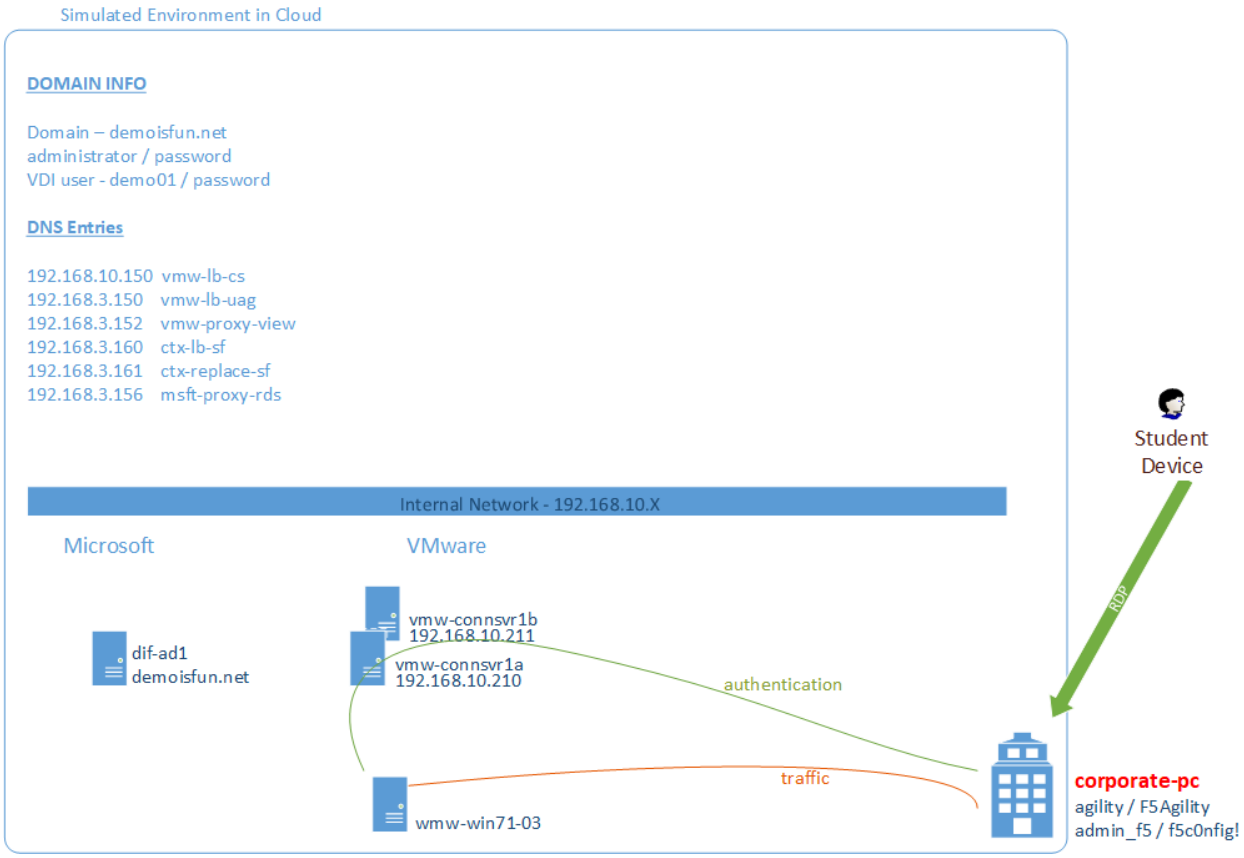


Fig. 2.1: *Accessing Internal Horizon Desktop*

6. After authenticated, double-click the **Agility** icon to launch Horizon Desktop
7. In the *Agility* desktop, open Notepad and type in something
8. Disconnect from *Agility* desktop by closing Horizon 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)
9. Open *Horizon* client again, reconnect to `vmw-connsvr1a.demoisfun.net` and open *Agility* desktop
10. *Notepad* should still be on the desktop with the text you input
11. Close the *Horizon* client. (press the **X** in Agility Toolbar)
12. Keep the RDP session open for Task 2

2.2 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)

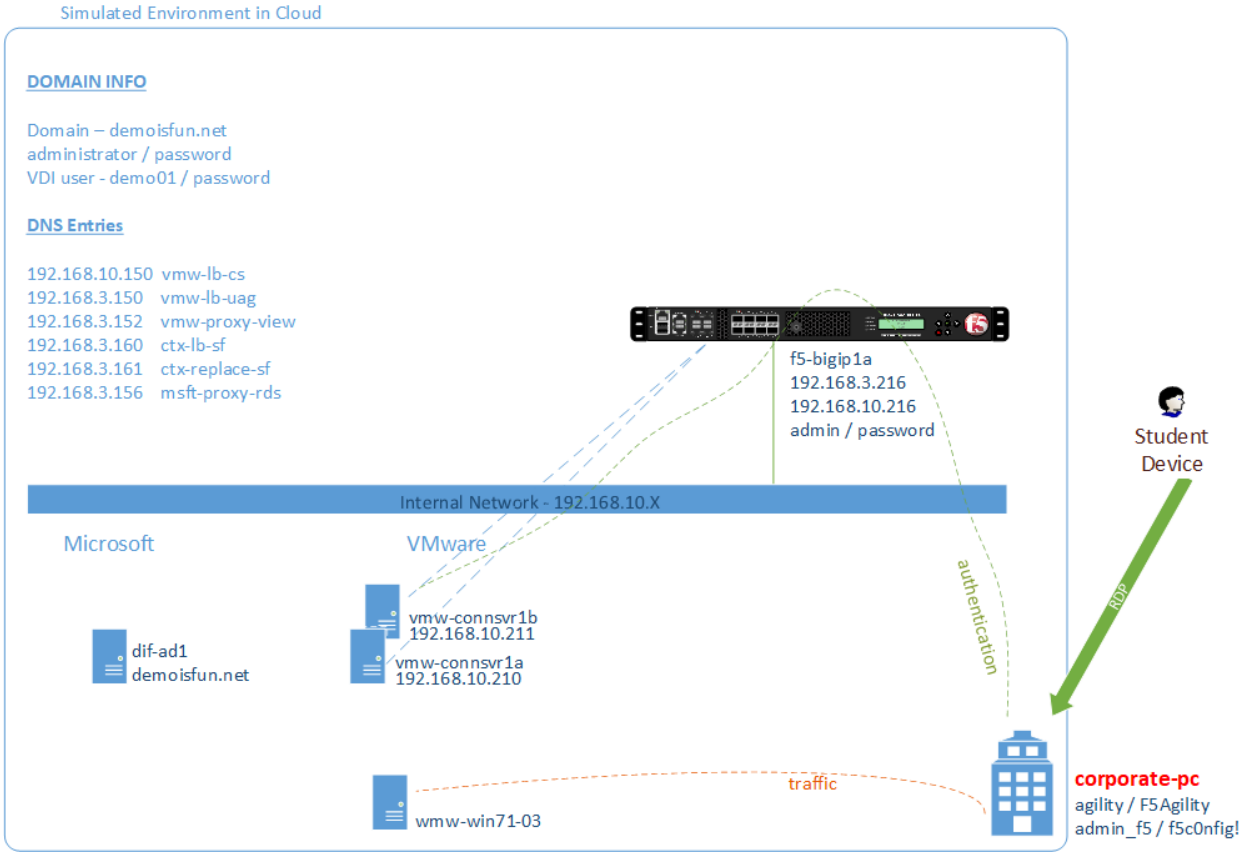


Fig. 2.2: *Load balance Connection Servers*

2.2.1 Deploy the iApp

1. From *"corporate-pc"*
2. Open IE to access the F5 Admin GUI at `https://f5-bigip1a.demoisfun.net`
   - Username: `admin`
   - Password: `password`
3. Create a new Application Service. On the left side menu
   - Go to **iApps -> Application Services -> Applications**
   - On the right side of the GUI, click **Create** button
   - In *Name* field, type in `lab2-lb-cs`
   - In *Template* pulldown, select `f5.vmware_view.v1.5.4`

Note: The tables for iApp questions list just the values that need to change

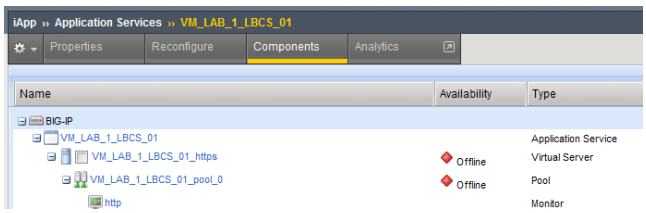
---

Welcome to the iAPP template for VMware Horizon	Please review
Big-IP Access Policy Manager	
Do you want to deploy BIG-IP Access Policy Manager?	*No, do not deploy BIG-IP Access. . .*
SSL Encryption	
How should the BIG-IP system handle encrypted traffic?	*Terminate SSL for clients, . . . (SSL-bridging)*
Which SSL certificate do you want to use?	*wild.demoisfun.net.crt* (Cert preloaded)
Which SSL private key do you want to use	*wild.demoisfun.net.key* (Key preloaded)
Virtual Servers and Pools	
What virtual server IP address. . . ?	`192.168.10.150`
What FQDN will clients use to access the View environment?	`vmw-LB-CS.demoisfun.net`
Which Servers should be included in this pool	`192.168.10.210` `192.168.10.211`
Application Health	
Create a new health monitor or use existing one?	`https`

4. Click the **Finished** button

2.2.2 View the objects which were created by the iApp

1. Click **Components** tab at the top of the page

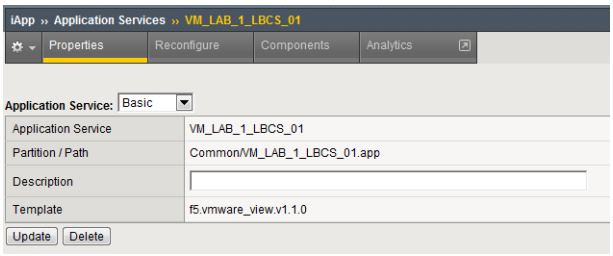


2. Is the Virtual server available?
3. Are the pool members available?

4. What is the node status? Why?
5. Note that a persistence profile was created
    - Click **lab2-lb-cs** to edit the object
    - Check **Match Across Services**
    - Click **Update**
    - Note the error at the top of the page
6. Return to *iApp -> Application Services -> lab2-lb-cs*
7. Review the remaining parameters (any questions)

2.2.3 View the properties of the iApp

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



2. In the *Application Service* pulldown, select **Advanced**
3. Note the *Strict Updates* checkbox is selected
    - Is this related to the error observed when editing the persistence profile?
    - What are the pro's and con's of unchecking this parameter?

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

1. From *"corporate-pc"*
2. Launch View client and connect to the Virtual Server just created with iApp
3. Click **New Server**
4. Type in the load balanced address `vmw-LB-CS.demoisfun.net`. (IP address will not work—Certificate contains demoisfun.net)
5. When prompted for credentials
    - Username: `demo01`
    - Password: `password`
6. Open the **Agility** desktop
7. Verify that the *Agility* desktop functions
8. Close the View client
9. Open a new Tab IE and browse to `https://vmw-LB-CS.demoisfun.net`

10. Click on **VMware Horizon HTML Access**
11. Log in
    - Username: `demo01`
    - Password: `password`
12. Open **Agility** desktop
13. At the Cert Warning, click “Continue to this website. . . ”
14. Verify that the Agility desktop functions
15. Close the IE *VMWare Horizon* tab

2.3 Task 3 – Access Horizon Desktop through the UAG Server

Access Horizon Desktop from external network through UAG. (External use case without F5 integration)

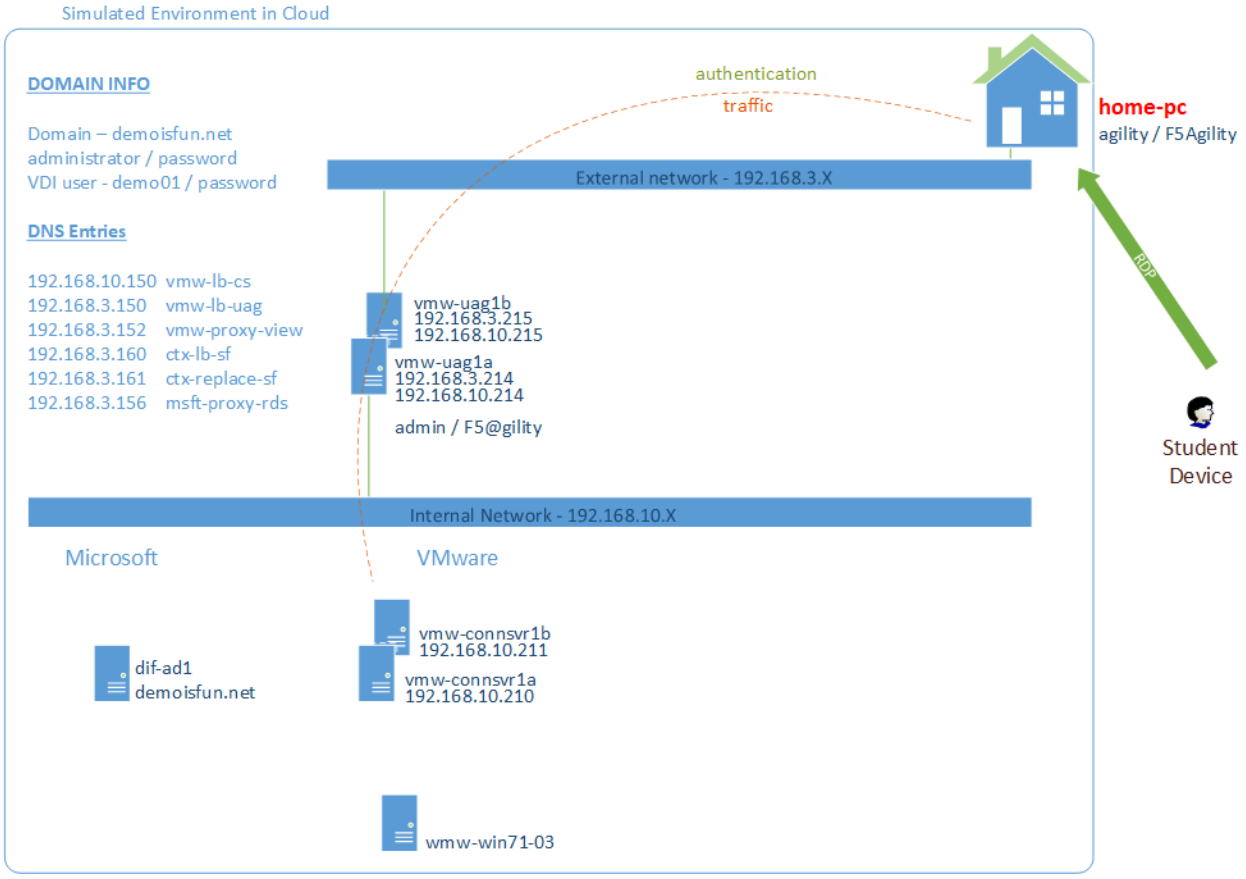
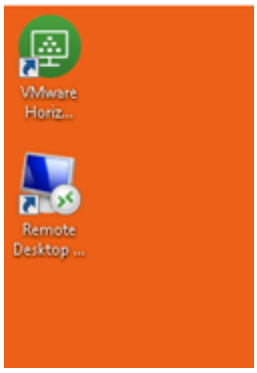


Fig. 2.3: *Access Horizon Desktop from external network*

1. From *“home-pc”*



2. On the desktop, Launch Horizon client and connect to the UAG
3. Click **New Server**
4. Type in the UAG address `vmw-uag1a.demoisfun.net`
5. When prompted for credentials
    - Username: `demo01`
    - Password: `password`
6. Open the **Agility** desktop
7. Close the *Horizon* client
8. To access *Horizon* desktop in IE, type in URL `https://vmw-uag1a.demoisfun.net`
9. Select **VMware Horizon HTML Access**
    - Username: `demo01`
    - Password: `password`
10. Open **Agility** desktop
11. Verify that the desktop functions
12. Close the IE *VMware Horizon* tab

2.4 Task 4 – Load Balance UAG Servers

Use the F5 iApp for VMware Horizon to configure a load balancing UAG's. This will increase the number of UAG servers available to external users and load balance access to these resources (External use case with F5 load balancing)

This environment load balances 2 external facing UAG Servers. UAG's do not require a one-to-one mapping to Connection Servers. The Connection Server LB VIP created in Task 2 enables higher availability to the overall application.

2.4.1 Deploy the iApp

1. From *"corporate-pc"*
2. Open IE to access the F5 Admin GUI at `https://f5-bigip1a.demoisfun.net`
    - Username: `admin`

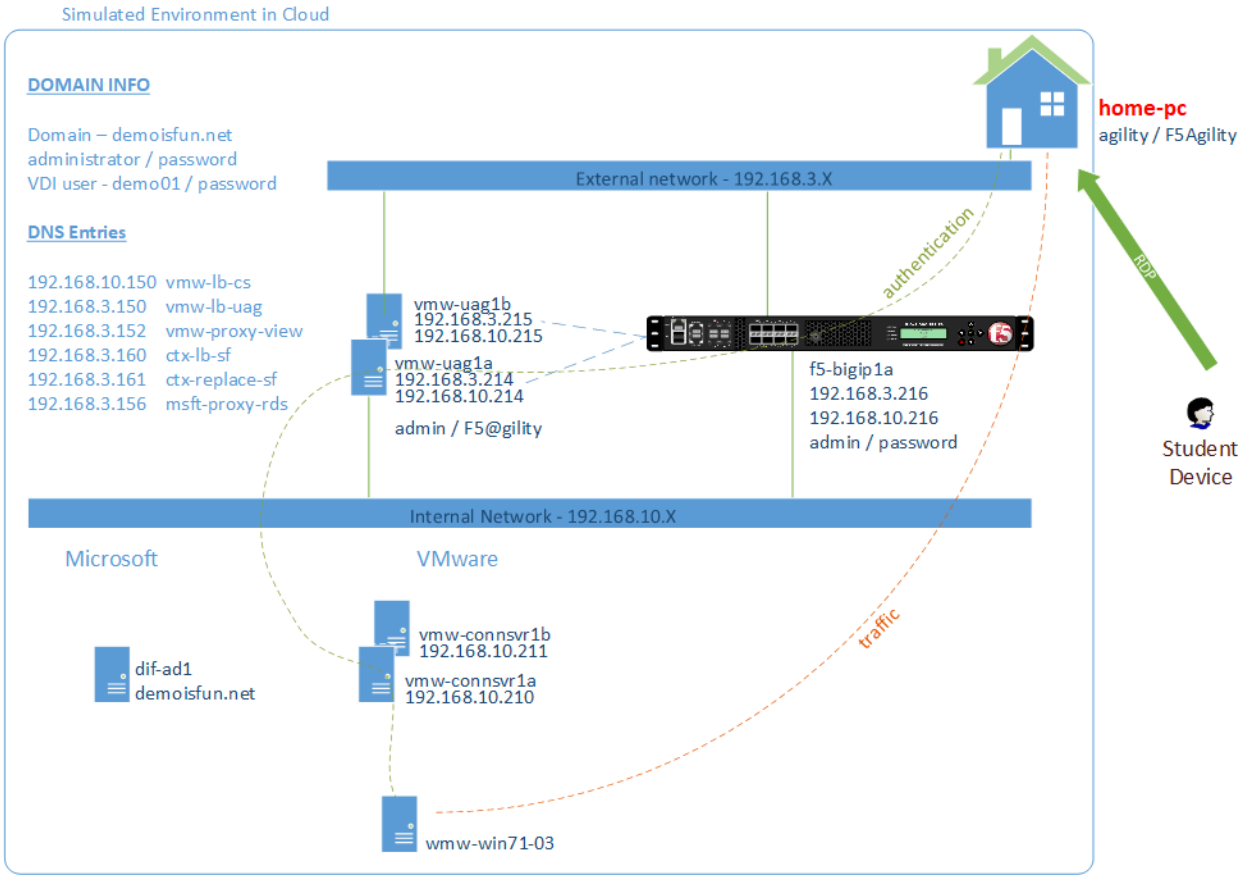


Fig. 2.4: *Load balance UAG's*

- Password: `password`

3. Create a new Application Service. On the left side menu
   - Go to **iApps -> Application Services -> Applications**
   - On the right side of the GUI, click the **Create** button
   - In the *Name* field, type in `lab2-lb-uag`
   - In the *Template* pulldown, select `f5.vmware_view.v1.5.4`

Big-IP Access Policy Manager	
Do you want to deploy BIG-IP Access Policy Manager?	*No, do not deploy BIG-IP Access Policy Manager*
SSL Encryption	
How should the BIG-IP system handle encrypted traffic?	*Terminate SSL for clients,...(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*
Virtual Servers and Pools	
What virtual server IP address...for remote, untrusted clients?	`192.168.3.150`
What FQDN will clients use to access the View environment	`vmw-LB-UAG.demoisfun.net`
Which Servers should be included in this pool	`192.168.3.214` `192.168.3.215`
Application Health	
Create a new health monitor or use existing one?	*https*

4. Click **Finished** button

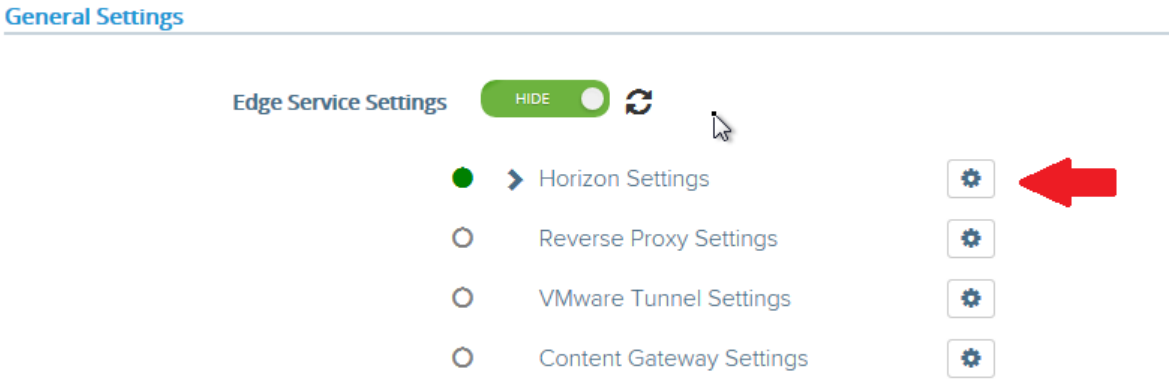
2.4.2 View the objects which were created by the iApp

1. Click **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)

2.4.3 Configure UAG to use load balance address

1. From *"corporate-pc"*
2. Open new tab in IE and go to *vmw-uag1a* administrative interface at `https://192.168.10.214:9443/admin`
3. Log in as
   - Username: `admin`
   - Password: `F5@gility`
4. On the right side, under *Configure Manually*, click **Select**

5. In *General Settings -> Edge Service Settings*, click the **Show** button



6. Next to *Horizon Settings*, click the **Gear**
7. In the *Blast External URL* field, type in `https://vmw-lb-uag.demoisfun.net:443`
8. In the *Tunnel External URL* field, type in `https://vmw-lb-uag.demoisfun.net:443`



9. Click **Save**
10. Make same changes for the other UAG *vmw-uag1b* at `https://192.168.10.215:9443/admin`

2.4.4 Test the UAG load balancing using Horizon and HTML5 client access methods

1. From *"home-pc"*
2. Launch View client and connect to the Virtual Server just created with iApp.
3. Click **New Server**
4. Type in the load balance address `vmw-LB-UAG.demoisfun.net`
5. When prompted for credentials
    - Username: `demo01`
    - Password: `password`
6. Open the **Agility** desktop
7. Verify that the *Agility* desktop functions
8. Close the View client
9. Open IE and browse to `https://vmw-LB-UAG.demoisfun.net`
10. Select **VMware Horizon HTML Access**
11. Log in
    - Username: `demo01`
    - Password: `password`
12. Open **Agility** desktop
13. Verify that *Agility* desktop functions
14. Close IE *VMware Horizon* tab

2.5 Task 5 – BIG-IP proxy View traffic in place of UAG

In this configuration, we will consolidate authentication, load balance and proxy View traffic on a single BIG-IP. This can bypass the UAG's to access View desktop from external network.

2.5.1 Deploy the iApp

1. From *"corporate-pc"*
2. Open IE to access the F5 Admin GUI at `https://f5-bigip1a.demoisfun.net`
    - Username: `admin`
    - Password: `password`
3. Create a new Application Service. On the left side menu
    - Go to **iApps -> Application Services -> Applications**
    - On the right side of the GUI, click the **Create** button
    - In the *Name* field, type in `lab2-proxy`
    - In the *Template* pulldown, select `f5.vmware_view.v1.5.4`

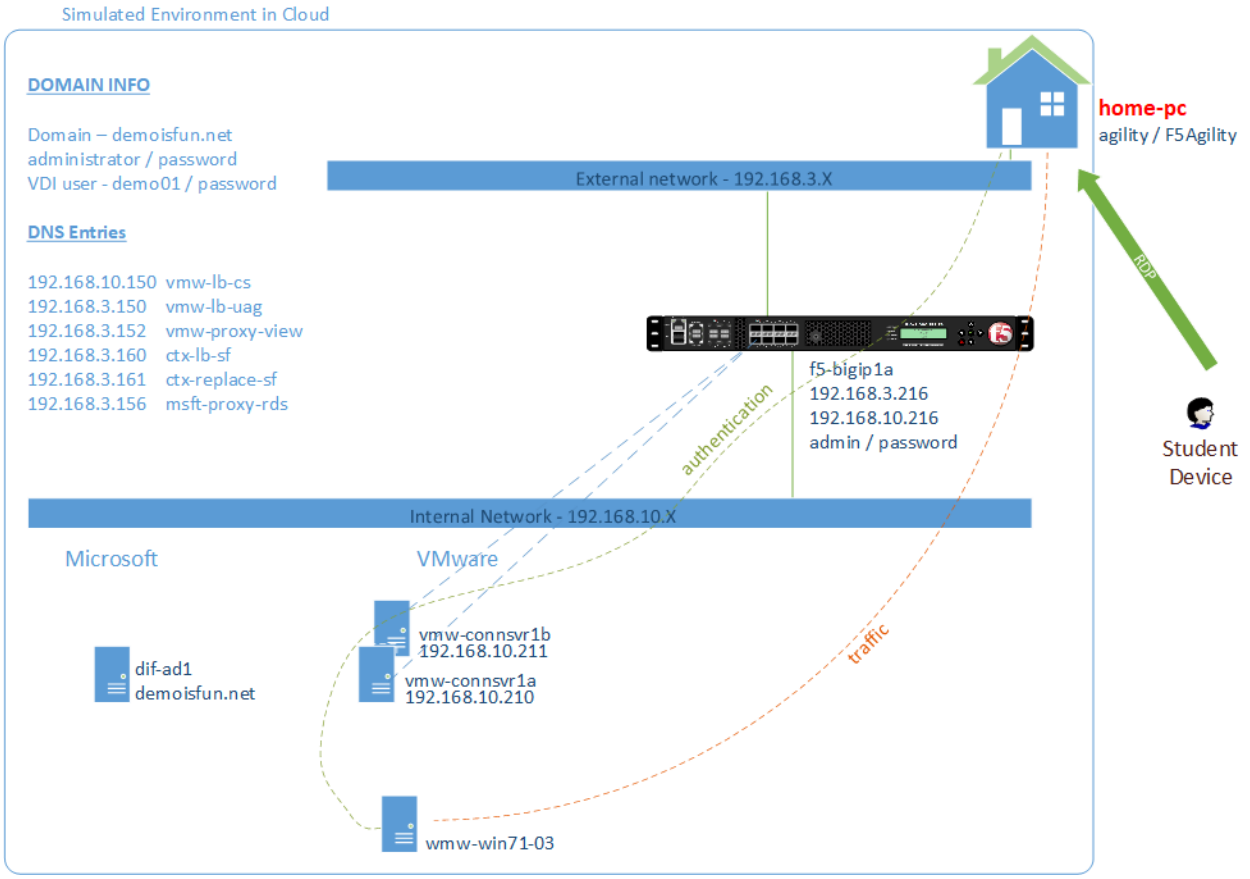


Fig. 2.5: *Consolidating authentication, load balance and proxy View on a single BIG-IP*

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. . . HTML5 client?	*Yes, support HTML 5 view clientless browser*
What is the NetBIOS domain name for your environment?	`demoisfun`
Create a new AAA Server object or select an existing one	*AD1*
SSL Encryption* section	
How should the BIG-IP system handle encrypted traffic?	*Terminate SSL for clients,. . . (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`
Virtual Servers and Pools	
What virtual server IP address. . . 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?	`192.168.10.210` `192.168.10.211`
Application Health	
Create a new health monitor or use existing one?	*https*

4. Click **Finished** button

2.5.2 View the objects which were created by the iApp

1. Click **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)

2.5.3 Test the APM webtop using Horizon and HTML5 client access methods

1. From *"home-pc"*
2. Launch **View Client**
   - Click **New Server**
   - Type in proxy address `vmw-PROXY-VIEW.demoisfun.net`
3. When prompted for credentials
   - Username: `demo01`
   - Password: `password`
4. Click **Agility** icon
5. Close the session by clicking the X in the upper toolbar
6. Open IE and browse to `https://vmw-PROXY-VIEW.demoisfun.net`

7. Select **VMware Horizon View HTML Access**
8. Enter credential
    - Username: `demo01`
    - Password: `password`
9. Click **Agility** to launch desktop
10. With APM Webtop, user has the option to choose client at launch time. Select **HTML5 Client**
11. Verify that the desktop functions
12. Close IE

3 Lab 3 - 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

3.1 Task 1 – Access XenDesktop without F5

1. From *corporate-pc*
2. Open IE and browse to Citrix Storefront at, `http://ctx-sf1a.demoisfun.net/Citrix/AgilityStoreWeb/`

Note: Storefront first launch takes a bit of time

---

1. When prompted for credentials
   - Username: `demoisfun\demo01`
   - Password: `password`
2. Click **Agility** to launch XenDesktop
3. Citrix *Desktop Viewer* launches and connects to XenDesktop
4. Verify virtual desktop function
5. In *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 IE

3.2 Task 2 – Load Balance StoreFront

3.2.1 Deploy the iApp

1. From *"corporate-pc"*

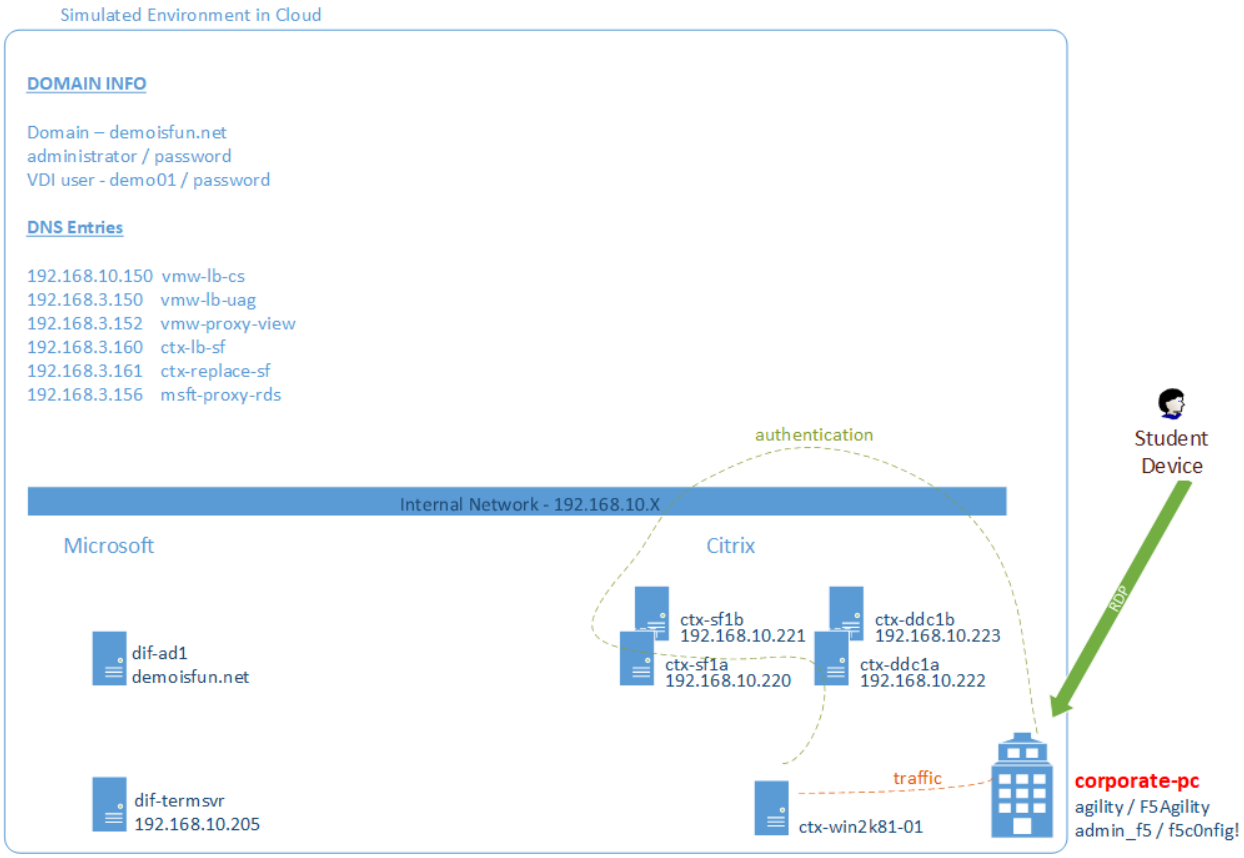


Fig. 3.1: *Access XenDesktop through StoreFront*

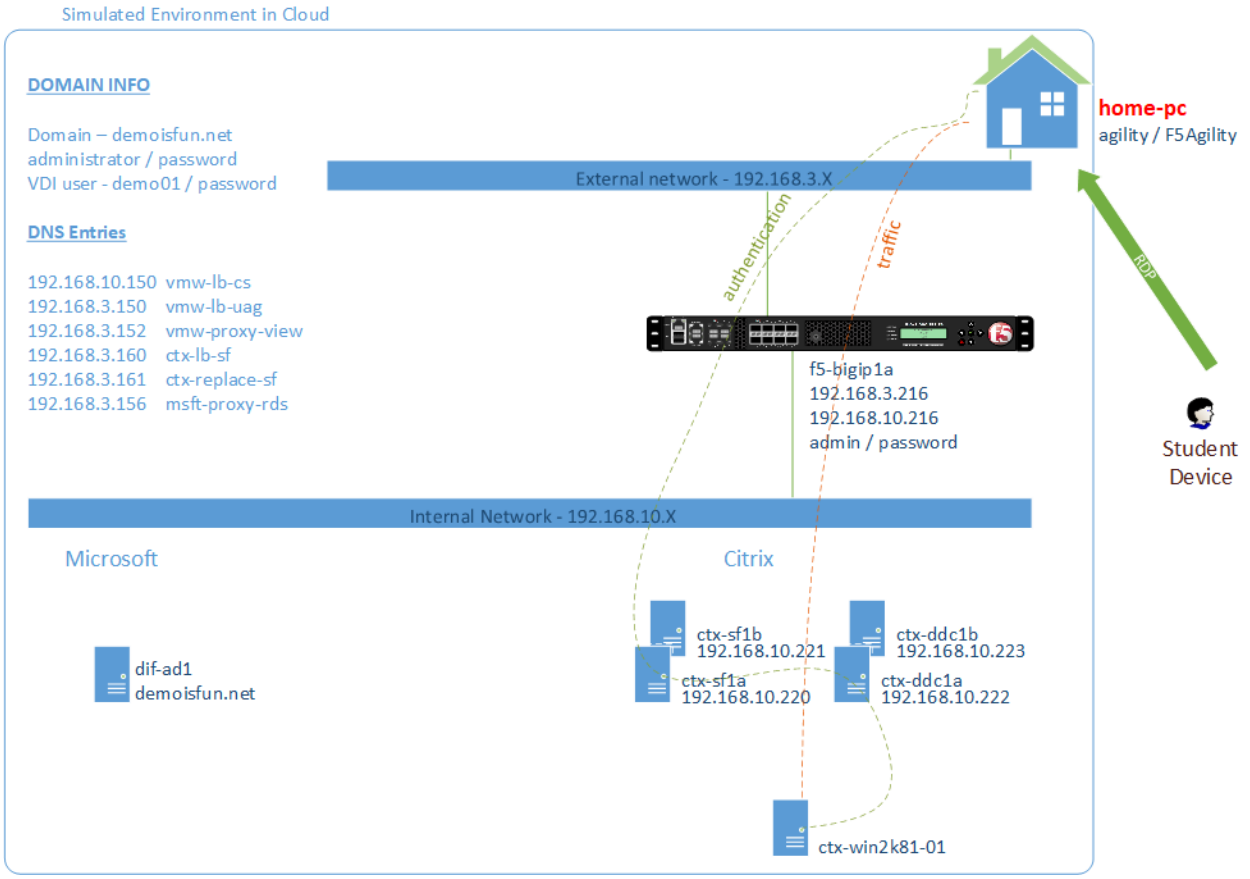


Fig. 3.2: *Load balance StoreFront*

2. Create a new Application Service.
    - **iApps -> Application Services -> Applications**
    - Click the **Create** button
    - In the *Name* field, type in `lab3-lb-sf`
    - In the *Template* pulldown, select **f5.citrix_vdi.v2.4.4**

Welcome to the iApp template for XenDesktop and XenApp	*Review this section*
General	
Use APM to securely proxy application (ICA)... Citrix environment?	*Yes, Proxy ICA traffic... with BIG-IP*
What is the Active Directory NetBIOS Domain Name... Citrix servers?	demoisfun
BIG-IP Access Policy Manager	
Do you want to replace Citrix Web Interface... with the BIG-IP system?	*No, do not replace...*
Create a new AAA object or select an existing one?	*AD1*
Virtual Server for Web Interface or StoreFront servers	
How should the BIG-IP system handle encrypted traffic to... servers?	*Terminate SSL for Clients... *(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... or the F5 Webtop?	`192.168.3.160`
Did you deploy Citrix StoreFront?	*Yes, ... StoreFront 3.0 or above*
What is the URI used on StoreFront... for XenApp or XenDesktop?	`/Citrix/AgilityStoreWeb/`
Web Interface or StoreFront servers	
What DNS name will clients use to reach the... StoreFront servers?	`ctx-LB-SF.demoisfun.net`
Which port... 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*
Virtual Server for XML Broker or Desktop Delivery Controller (DDC) Servers	
What IP address do you want to use for the... DDC farm virtual server?	`192.168.10.161`
How will requests from the Web Interface or StoreFront servers arrive?	*XML Broker... requests will arrive unencrypted (HTTP)*
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*

3. Click **Finished** button

3.2.2 Test Connectivity

1. From *"home-pc"*

2. OpenIE and go to the StoreFront load balanced address, `http://ctx-lb-sf.demoisfun.net`
3. When prompted for credentials
    - Username: `demo01`
    - Password: `password`
4. Click **Agility** to launch XenDesktop
5. In the *Citrix Agility* desktop, click **Start -> Disconnect**
6. Log off StoreFront using the **01 Demo** pulldown in the upper right corner

3.3 Task 3 – BIG-IP Replaces StoreFront

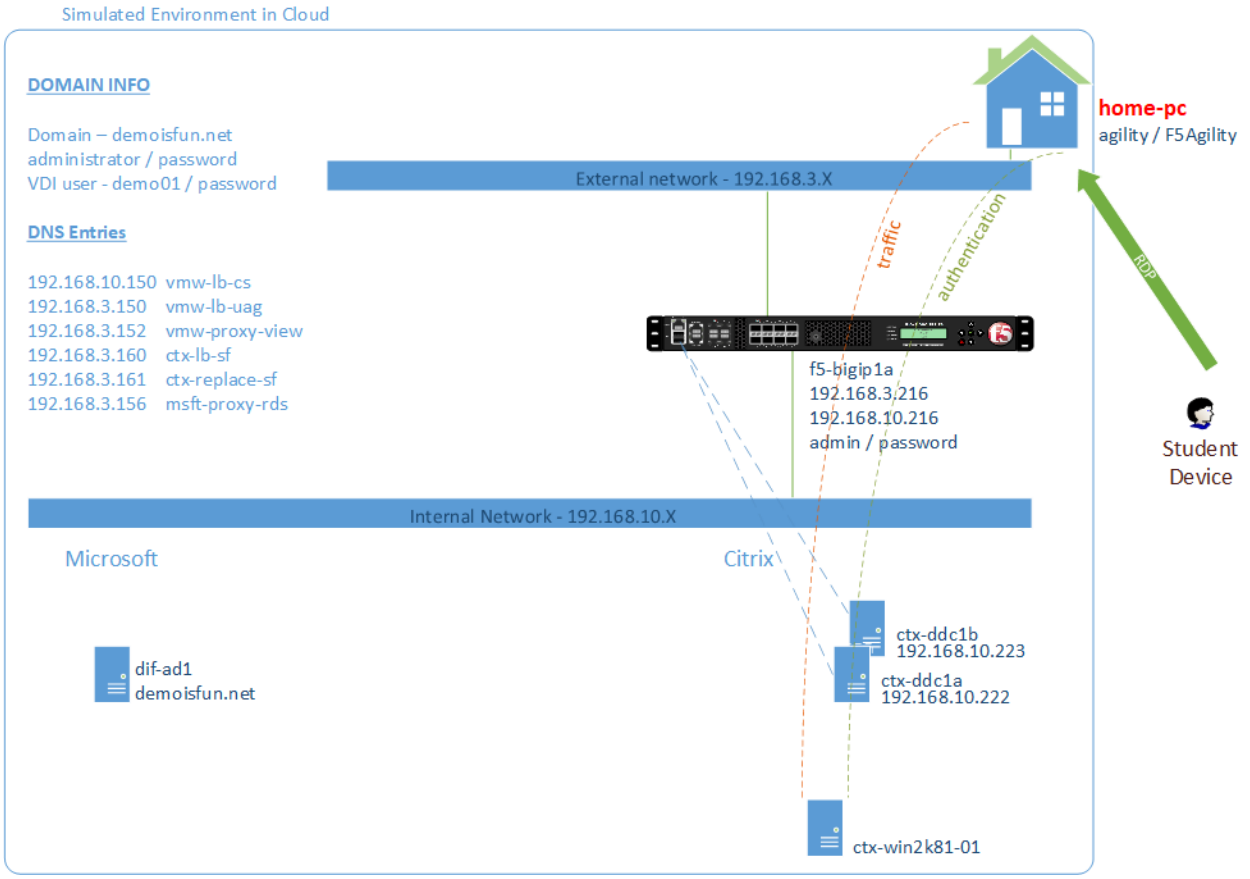


Fig. 3.3: *BIG-IP replaces StoreFront*

3.3.1 Deploy the iApp

1. From *"corporate-pc"*
2. Create a new Application Service.
    - **iApps -> Application Services -> Applications**

- Click **lab3-lb-sf**
- Click **Reconfigure** link near the top

BIG-IP Access Policy Manager	
Do you want to replace Citrix Web Interface. . . with the BIG-IP system?	*Yes, replace Citrix. . .*

3. Scroll through the template and note that the storefront pool members are no longer present (not needed)
4. Press the **Finished** button

3.3.2 Test Connectivity

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

4 Lab 4 - Proxy for Microsoft RDS

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

4.1 Task 1 – Access Terminal Server from external network

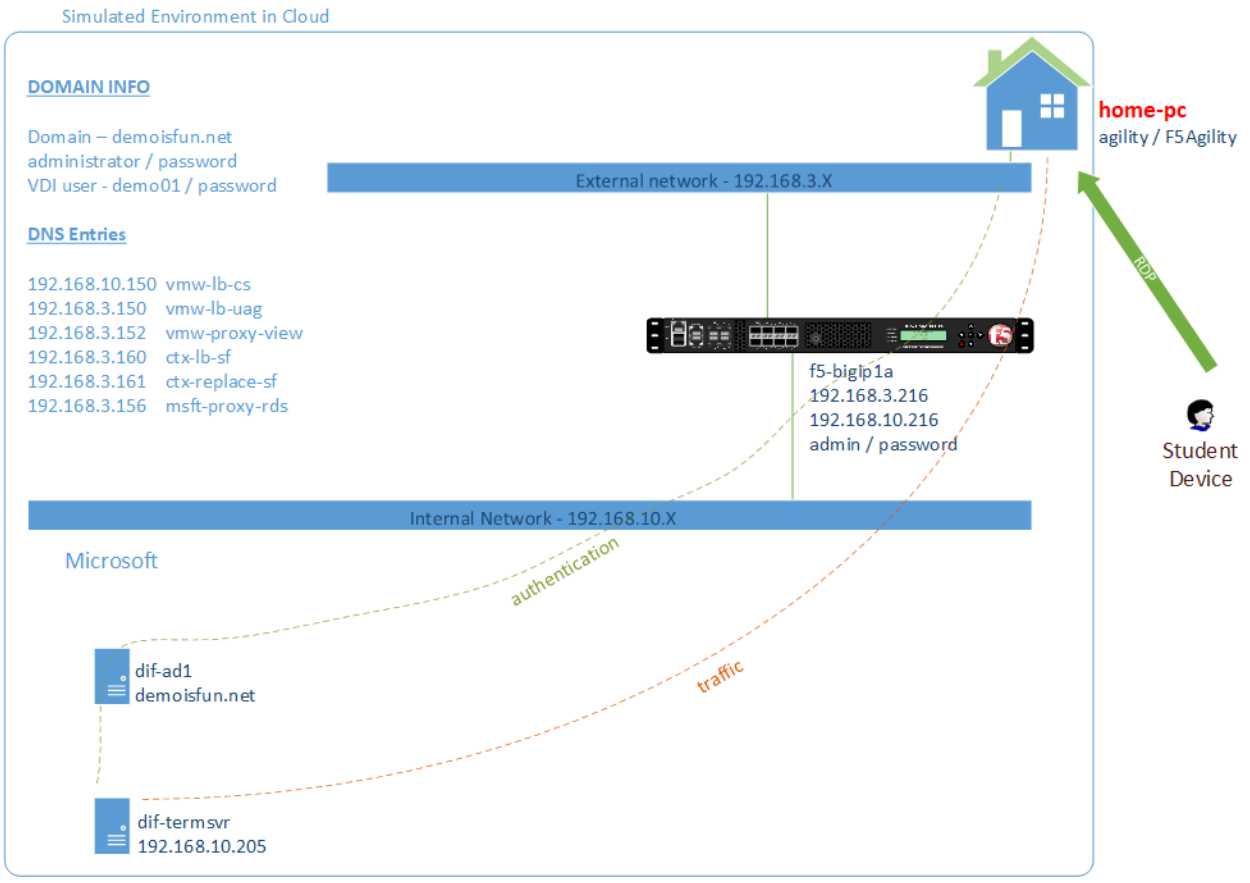


Fig. 4.1: *BIG-IP proxy RDP connection*

4.1.1 Create and bind NTLM Machine Account

1. From “corporate-pc”
2. Open IE to access F5 Admin GUI at, `https://f5-bigip1a.demosifun.net`
   - Username: `admin`
   - Password: `password`
3. Create on BIG-IP and bind to an NTLM Machine Account. On the left menu,
   - Click **Access -> Authentication -> NTLM -> Machine Account**
   - Click the **Create** button on the upper right corner

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

4. Click the **JOIN** button to create the machine account

4.1.2 Deploy iApp

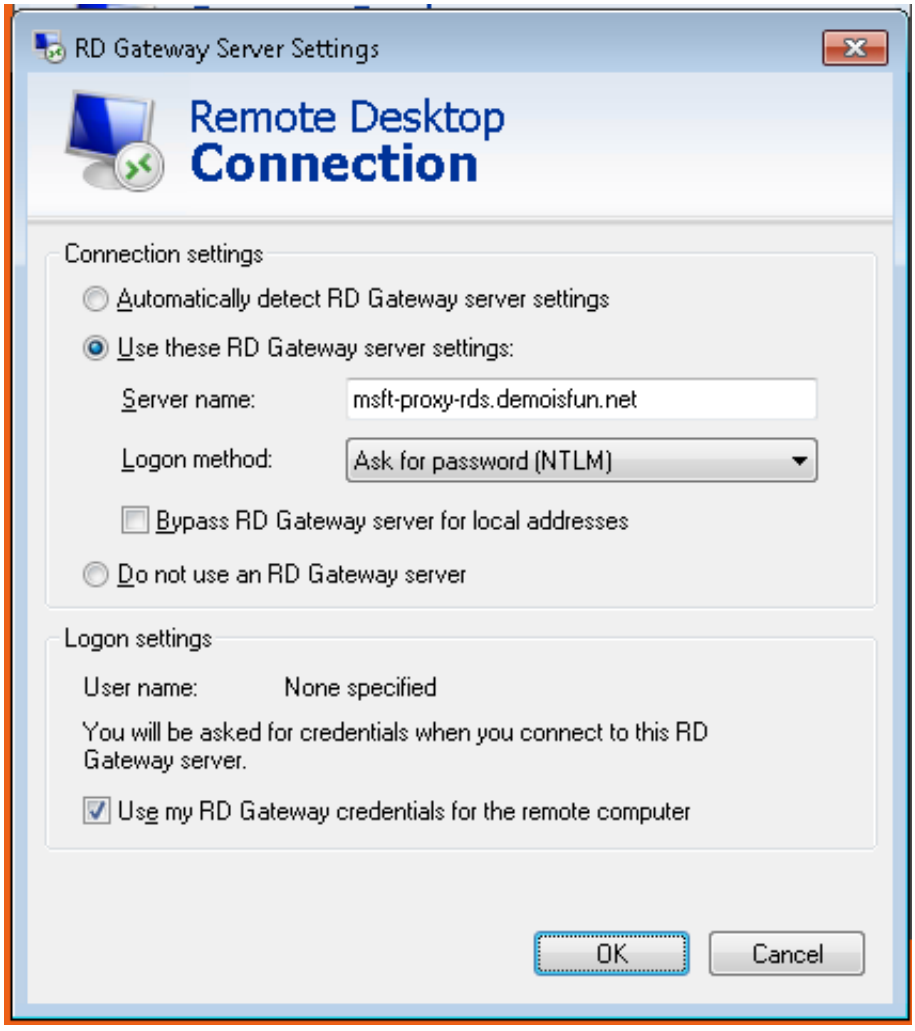
1. Create a new Application Service.
2. **iApps -> Application Services -> Applications**
3. Click the **Create** button
4. In the Name field, type in `lab4-rds`
5. In the Template pulldown, select `f5.microsoft_rds_remote_access.v1.0.3`

Welcome to the iApp template for Remote Desktop Gateway	*Please review*
Template Options	
Do you want to deploy BIG-IP APM as an RDP proxy?	*Yes, deploy BIG-IP Access Policy...*
Access Policy Manager	
Do you want to create... or use an existing AAA server?	*AD1*
Which NTLM machine account... for Kerberos delegation?	*AD1-f5-bigip1a*
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`
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. Click **Finished** button

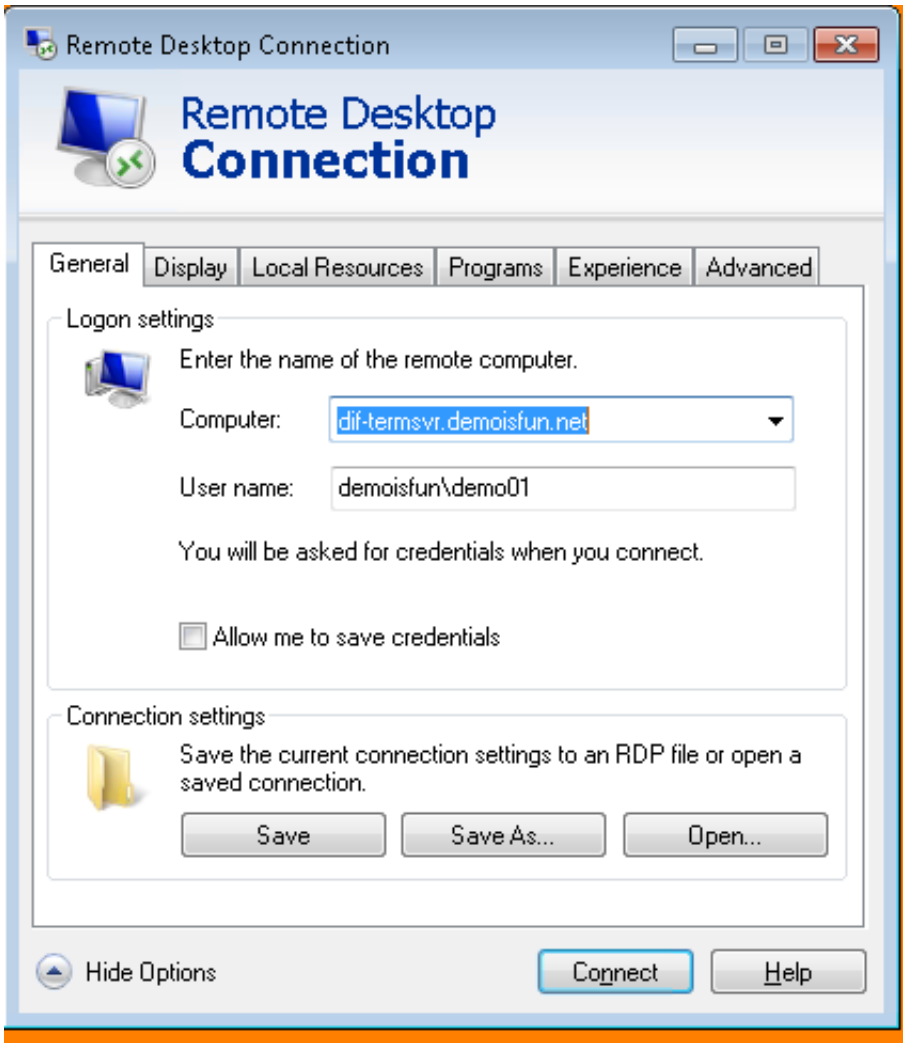
4.1.3 Test the RDS proxy functionality using RDS Client

1. From *"home-pc"*
2. Launch RDS client (on desktop)
3. Click **Show Options** pulldown
4. Click **Advanced** tab
5. Click **Settings** button
6. In *"RDS Gateway..."* window,
   - Select **"Use these RD Gateway..."** radio button
   - 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
   - Select **"Use my RD Gateway credential..."** checkbox
   - Click **OK**

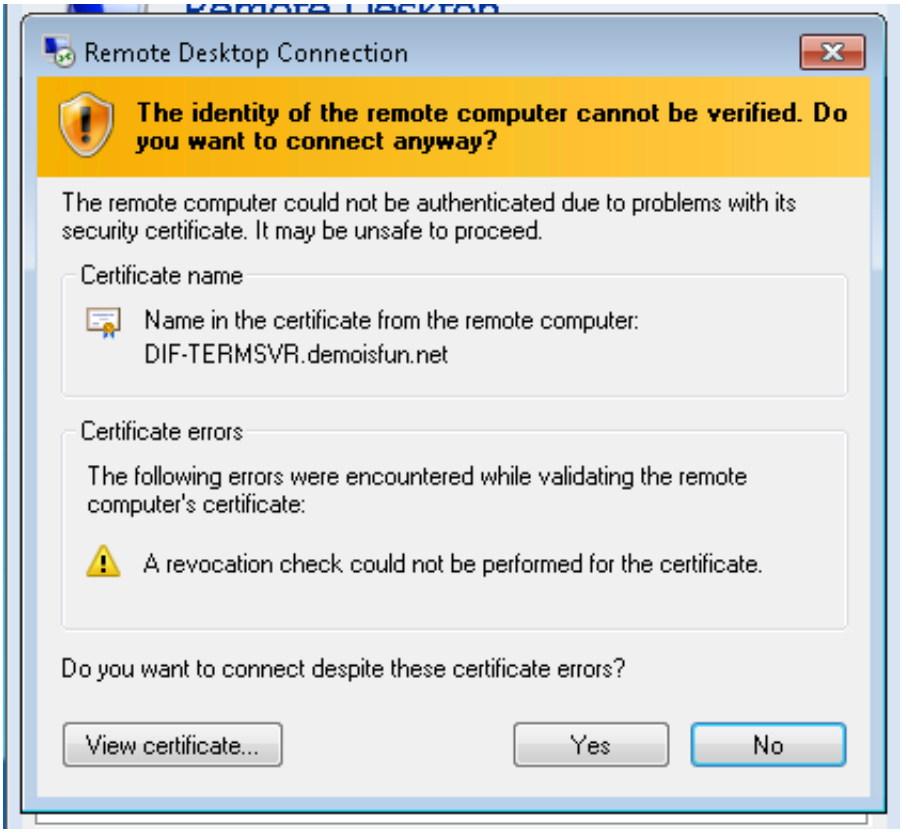


7. Under *"General"* tab, in *"Computer"* field, type in the name of the host you want to RDP to which is `dif-termsvr.demoisfun.net`
   - In *User name* field, type in `demoisfun\demo01`

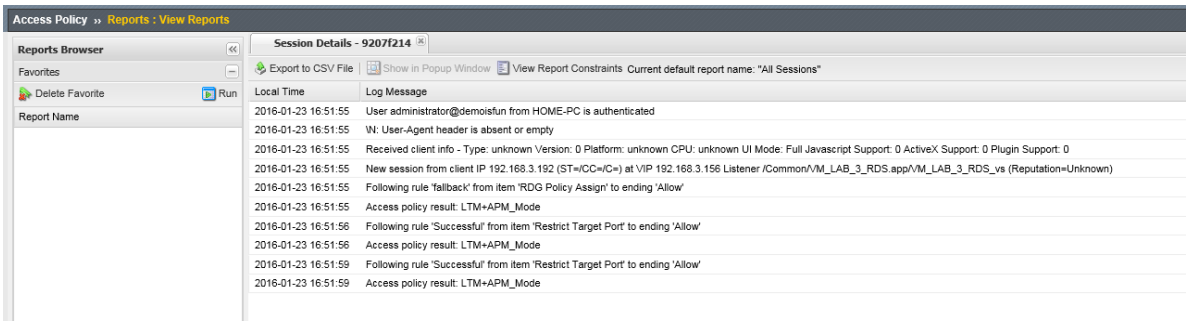
- Click **Save**
- Click **Connect**



8. When prompted for credentials
    - Username: `demo01`
    - Password: `password`
9. Click **Yes** to the Certificate warning



10. You are connected to dif-termsvr.demoisfun.net server
11. You can verify this connection through the BIG-IP. From *"corporate-pc"*, open IE to Connect to BIG-IP GUI
12. On the left side menu, click **Access -> Overview -> Active Sessions**
13. Click on the session to view details



14. Log off RDS session by clicking **Start -> Logoff**

5

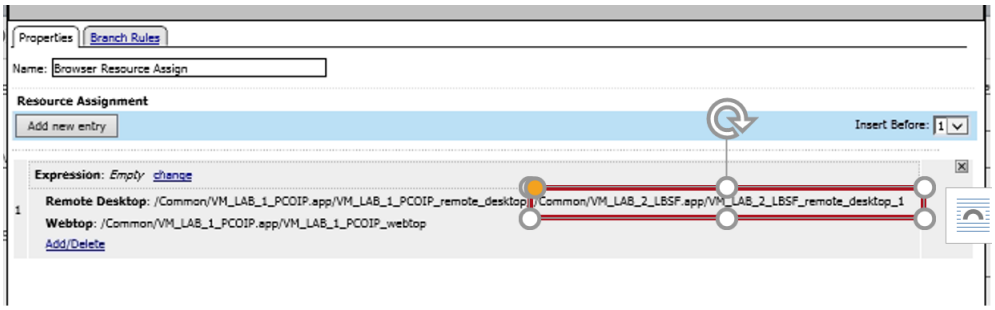
Lab 5 - Consolidate VDI Access

This lab will leverage the APM access policies created in prior labs to build a unified webtop with access to Vmware View and Citrix

5.1 Task 1 – Build a VIP with an Access Policy allowing access to VMware and Citrix

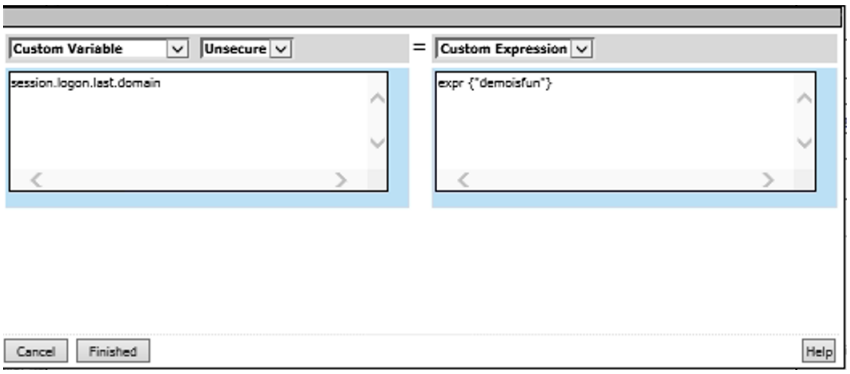
1. From *"corporate-pc"*
2. Open F5 config GUI
3. Disable *Strict Updates* for the *lab2-proxy* Application
   - Go to **iApps -> Application Services**
   - Click **lab2-proxy**
   - Click **Properties** tab
   - In *Application Service* pulldown, select **Advanced**
   - Uncheck **Strict Updates** checkbox
   - Click **Update** button
4. To save lab time, we removed "Strict Updates" so we can copy *lab2-proxy* Access profile objects
   - Go to **Access -> Profiles/Policies -> Access Profiles. . .**
   - Click "Copy" hyperlink on the *lab2-proxy* line
   - In the "Copied Profile Name" field, type in `lab5-webtop`
   - Click "Copy" button
5. View the characteristics of the *lab5-webtop* and *lab3-lb-sf* Access policies. To consolidate Citrix and VMware access, the subsequent steps will incorporate the components from Citrix policy into the copy of the VMware policy.
   - Go to **Access -> Profiles/Policies -> Access Profiles. . .**
   - On the *lab2-proxy* line, click **Edit** link. Review components and click **Close**
   - on the *lab3-lb-sf* line, click **Edit** link. Review components and click **Close**

6. Open *lab5-webtop* VPE
    - Go to **Access -> Profiles/Policies -> Access Profiles. . .**
    - On the *lab5-webtop* line, click **Edit** link and review.
7. Add Citrix to the *Browser Resource Assign* on the *Full or Mobile Browser* branch
    - Click **Browser Resource Assign** object on the right end or the branch
    - In the *Browser Resource Assign* pop-up, click **Add/Delete**
    - Click **Remote Desktop. . .** tab
    - Select /**Common/lab3-lb-sf.app/lab3-lb-sf_remote_desktop_1** checkbox. (Both check boxes should be selected)
    - Click **Update** button
    - Click **Save** button



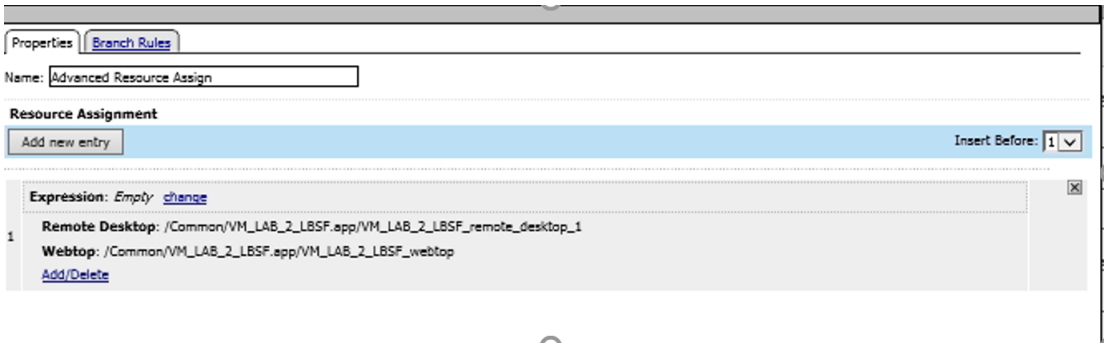
8. Add a branch for the *Citrix Receiver* to *Client Type*
    - Click **Client Type** object
    - Click **Branch Rules** tab
    - Click **Add Branch Rule** button
    - In *Name* field, replace *Branch Rule 1* with `Citrix Receiver`
    - Under *Citrix Receiver*, click **change** link
    - Click **Add Expression** button
    - In *Agent Sel* pulldown, select **UI Mode**
    - In *UI Mode is* pulldown, select **Citrix Reciever**
    - Click **Add Expression** button
    - Click **Finished** button
    - Click **Save** button (this takes a while)
9. Add a *Logon Page* object to the *Citrix Receiver* branch
    - On the *Client Type, Citrix Receiver* branch, click the **"+"**
    - In the *Logon* tab, select **Logon Page**
    - Click **Add Item** button
    - Review the default settings
    - Click **Save** button
10. Add *Domain Variable Assign* object to the *Citrix Receiver* branch

- On the *Logon Page, fallback* branch, click the "**+**"
- Click **Assignment** tab
- Select **Variable Assign** radio button
- Click **Add Item** button
- Click **Add new entry** button
- Click **change** link
- On the left panel, below *Custom Variable – Unsecure*, type in `session.logon.last.domain`
- On the right panel, below *Custom Expression*, type in `expr {"demoisfun"}`
- Click **Finished** button
- Click **Save** button

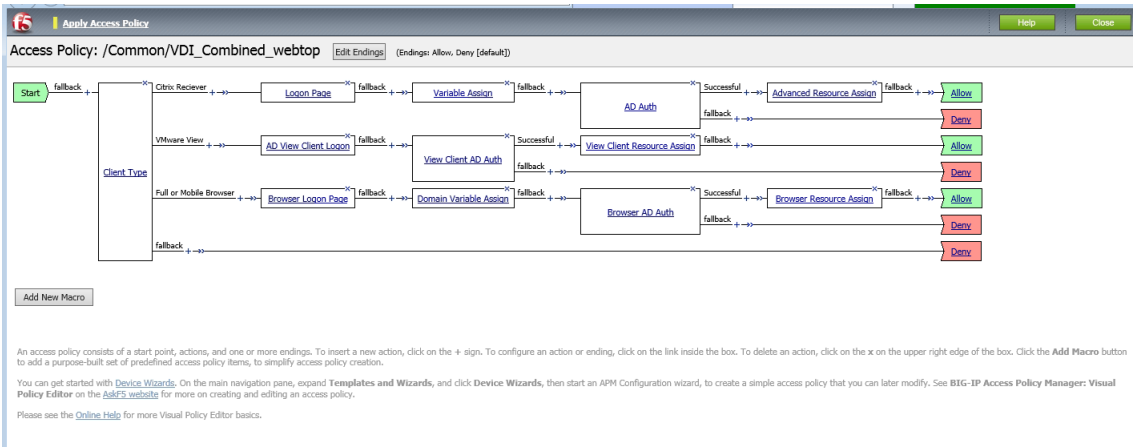


11. Add an *AD Auth* object to the Citrix Receiver branch
    - On the *Variable Assign, fallback* branch, click "**+**"
    - Click **Authentication** tab
    - Select **AD Auth** radio button
    - Click **Add Item** button
    - In the *Server* pulldown, select /**Common**/**AD1**
    - Click the **Save** button
12. Add an *Advanced Resource Assign* object to the Citrix Receiver branch
    - To the right of *AD Auth, Successfull* branch, click the "**+**"
    - Click **Assignment** tab
    - Select **Advanced Resource Assign** radio button
    - Click **Add Item** button
    - Click **Add new entry** button
    - Click **Add**/**Delete** link
    - Click **Remote Desktop. . .** tab
    - Select /**Common/lab3-lb-sf.app/lab3-lb-sf_remote_desktop_1** check box
    - Click **Webtop. . .** tab
    - Select **Common/lab3-lb-sf.app/lap3-lb-sf_webtop** radio button

- Click **Update** button
- Click **Save** button
- To the right of *Advanced Resource Assign, fallback* branch, click **Deny**
- Select **Allow** radio button
- Click **Save** button
- On the upper right corner, click **Close** the VPE. Click **YES** on the IE pop-up



13. Apply the access policy
    - On the upper left corner of the main F5 GUI, click **Apply Access Policy**
    - Select all policies, click **Apply**
    - Verify that all Access policies status is Green (refresh browser if necessary)



14. Create a Virtual Server for PCOIP traffic
    - Go to **Local Traffic -> Virtual Servers -> Virtual Server List**
    - View the configuration of the *lab2-proxy_pcoip_udp* Virtual Server (VS). We will replicate this configuration using the IP of the new VIP we created for VDI access (Hint—Open an additional browser window connected to F5-bigip1a.demoisfun.net. This will allow you to display different VIPs in the same device)
    - Go to **Local Traffic -> Virtual Servers -> Virtual Server List**
    - Click **Create** button in the upper right section of the GUI
    - Configure the VIP with the variables below

General Properties	
Name	`lab5-pcoip`
Destination Address/Mask	`192.168.3.157`
Service Port	`4172`
Configuration	
Protocol	*UDP*
Source Address Translation	*Auto Map*
Access Policy	
Application Tunnels (Jave & Per-App VPN)	Enabled - **Checked**

- Click **Finished** button

15. Create a combined VS for Citrix and VMware connectivity
    - Go to **Local Traffic -> Virtual Servers -> Virtual Server List**
    - Click **Create** button in the upper right section of the GUI
    - Configure the VIP with the variables below
16. VIP Config Parameters

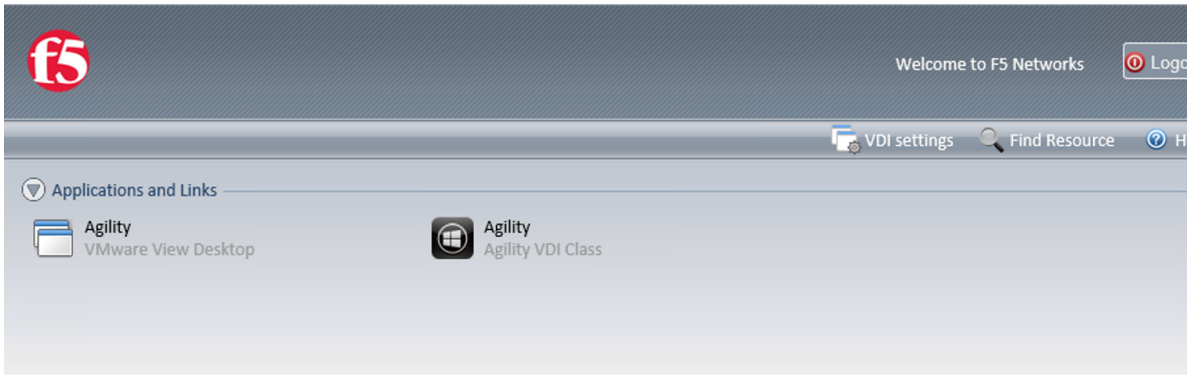
General Properties	
Name	`lab5-vdi`
Destination Address/Mask	`192.168.3.157`
Service Port	`443`
Configuration	
HTTP Profile	*http*
SSL Profile (Client)	*lab2-proxy_client_ssl*
SSL Profile (Server)	*serverssl*
Source Address Translatio	*Auto Map*
Access Policy	
Access Profile	lab5-webtop_webtop
Connectivity Profile	lab2-proxy_connect
VDI Profile	vdi

17. Click **Finished** button

5.1.1 Test Connectivity

1. From *"home-pc"*
2. Open IE and browse to `https://vdi.demoisfun.net`. Note this address has been configured in DNS to resolve to the VIP 192.168.3.157
3. When prompted for credentials
    - Username: demo01
    - Password: password
4. APM webtop is displayed with - Agility - Vmware View Desktop - Agility - Agility VDI Class (Citrix)
5. Click **Agility - Agility VDI Class** to launch XenDesktop
6. In *Select client** pop-up, click **Citrix Receiver** button
7. Verify that desktop is functional

8. In Citrix Agility desktop, click **Start -> Disconnect**. This will return you to APM webtop
9. Click **Agility - Vmware View Desktop**
10. In *Select client* pop-up, click **VMware Horizon** button
11. Verify that the VMware desktop functions
12. Close *View* client



6

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 !!!



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: f5j-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.