IIS Web Serving and Server Monitoring

Jordan Brown

Overview

In this Assignment I will be using IIS to configure 4 sites to their appropriate specifications, after making the sites I will be evaluating a monitoring service.

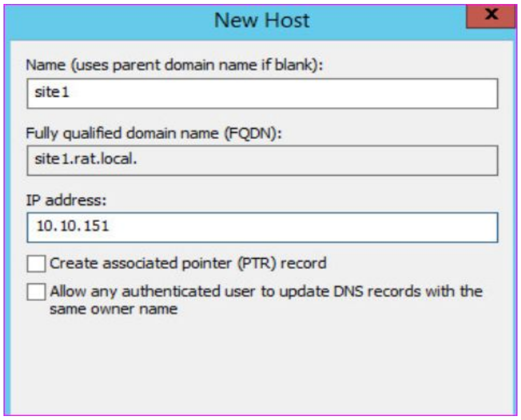
IP Allocation

10.10.1.51 Site1
10.10.1.52 Site2
10.10.1.53 Site3
10.10.1.54 admins(Site4)

IIS Configuration

On whichever server you're wanting to host the IIS server go to server manager and install the IIS role.

Making an (A) record with the allocated IP's.
On server manager go to **Tools** > **DNS** > **Forward Lookup Zones** > **rat.local**, right click on rat.local and select **New Host (A or AAAA)** call this one **site1** and give an IP address of **10.10.1.51** and click **add host**. Repeat this for the other 3 sites.



New Host

Name (uses parent domain name if blank):
site1

Fully qualified domain name (FQDN):
site1.rat.local.

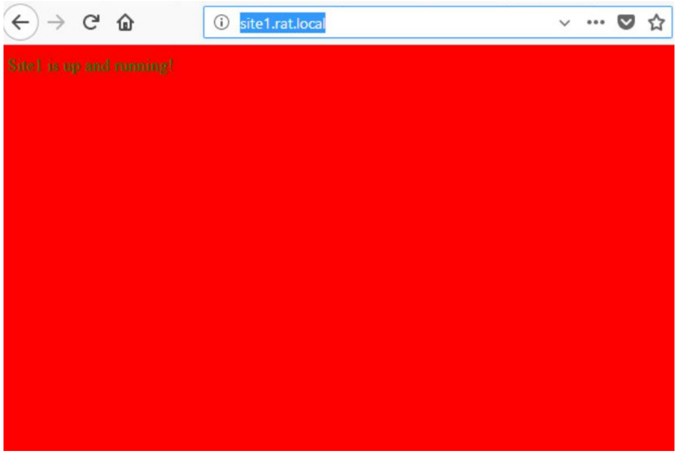
IP address:
10.10.151

□ Create associated pointer (PTR) record
□ Allow any authenticated user to update DNS records with the same owner name

Now you are ready to begin creating the sites!

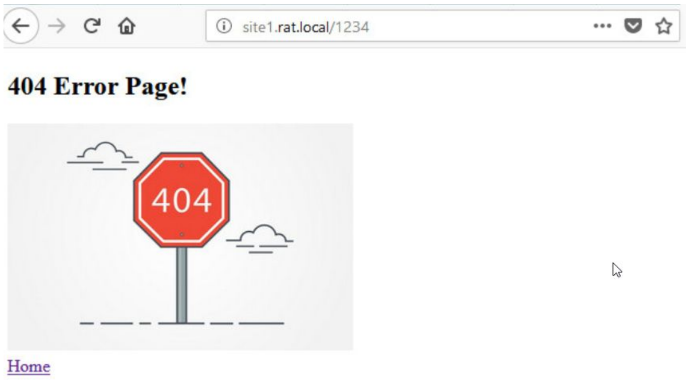
IIS Site1 Configuration

Create a new site called site1, which will be site1.rat.local in the browser(it's a subdomain). To disable the indexing first create a custom HTML page you want to be your front page and put it in your site1 folder, name it **index.html**. Now to make sure IIS will recognise it above all others as the default go to **Default Document** inside site1 on IIS. Click on **index.html** and on the side click **Move up** until it reaches the top(if you receive a warning prompt hit **Ok**). Now in **Directory Browsing** on the dashboard under **Actions** click **Disable** this will then turn off indexing for this site.



Site1 is up and running!

To set up an Error page first make a custom **Error.html** then go to **Error Pages** inside Site1 edit then edit the status code 404 Error Page. inside Edit choose the 2nd radio box **Execute a URL** on this site type in **/Error.html** and click **Ok** to save changes. Now click on **Edit Feature Settings…** choose the first radio box **Custom error pages** and click **Ok** to save your changes. Now when you type anything besides existing URLs for your site1 it should return the error page (ie. site1.rat.local/1234).



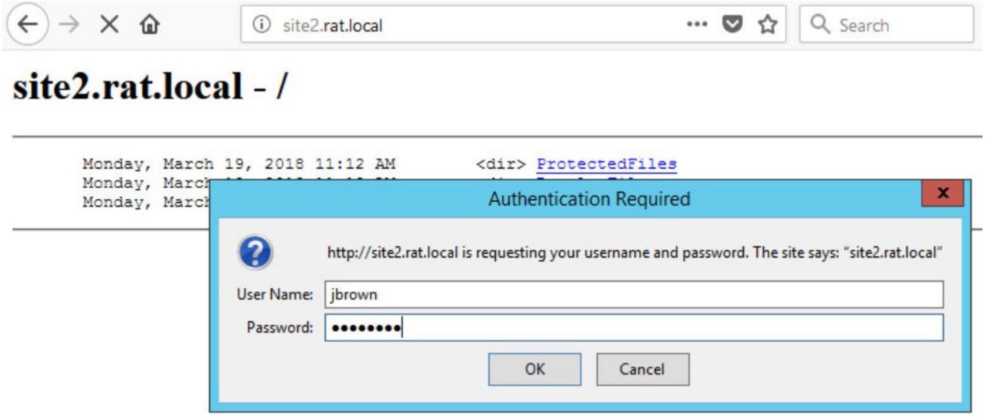
404 Error Page!

Home

IIS Site2 Configuration

First create a folder named site2 inside the folder add another folder called RegularFiles and ProtectedFiles inside site2 in IIS then create an HTML file in each of the folders (Protected.html, Regular.html). Inside IIS click on site2 go to **Directory Browsing** and enable it. Now go to **Authentication** and Enable **Basic Authentication**, make sure **Anonymous Authentication** is disabled.

Now we can access the ProtectedFiles with only domain user accounts.



site2.rat.local

site2.rat.local - /

```
Monday, March 19, 2018 11:12 AM        <dir> ProtectedFiles
Monday, March
Monday, March
```

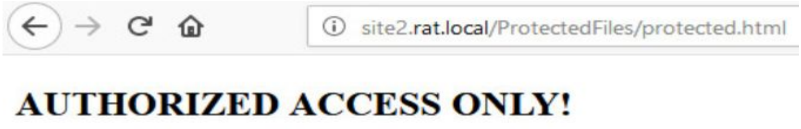
Authentication Required

http://site2.rat.local is requesting your username and password. The site says: "site2.rat.local"

User Name: jbrown

Password: ••••••••

Protected.html



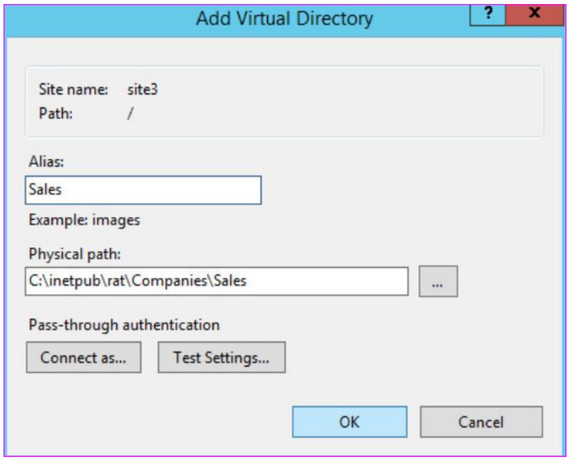
site2.rat.local/ProtectedFiles/protected.html

AUTHORIZED ACCESS ONLY!

IIS Site3 Configuration

Inside IIS right click **Sites** and click **add website** call the site **site3**
Browse to the physical path of the site and click **Ok**. Give it an IP address in the drop down box and give it a host name of **site3.rat.local**. And click **Ok.**

Once the site is created right click on it and click **add Virtual directory** give this one an **Alias** of sales and find the physical path for the sales folder and click **Ok**.



Add Virtual Directory

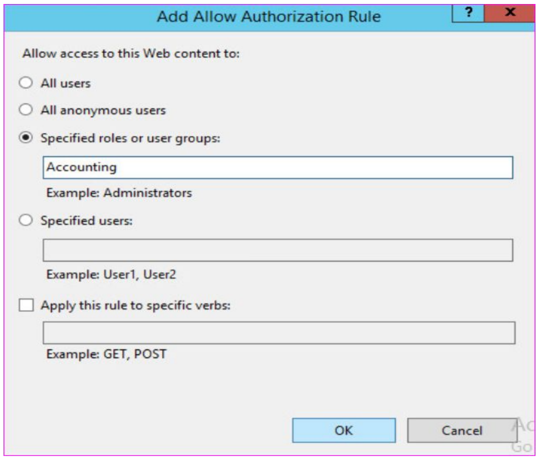
Site name: site3
Path: /

Alias:
Sales
Example: images

Physical path:
C:\inetpub\rat\Companies\Sales

Pass-through authentication

Now click on **Site3** > **Accounting** > **Authentication** disable **Anonymous Authentication** and enable **Windows Authentication**. Back on Accounting Home go to **Authorization Rules**, remove the inherited rule and right click **Add Allow Rule**. select **Specified roles or user groups** and type in **Accounting** and click **Ok**.



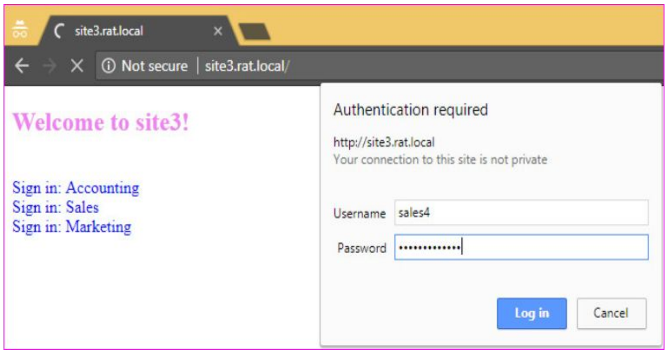
Add Allow Authorization Rule

Allow access to this Web content to:

○ All users
○ All anonymous users
● Specified roles or user groups:
Accounting
Example: Administrators
○ Specified users:
Example: User1, User2
□ Apply this rule to specific verbs:
Example: GET, POST

Repeat this for the accounting and marketing virtual directory.

Now when you go to site3 on the win8 client try logging on to the virtual directories.



Welcome to site3!

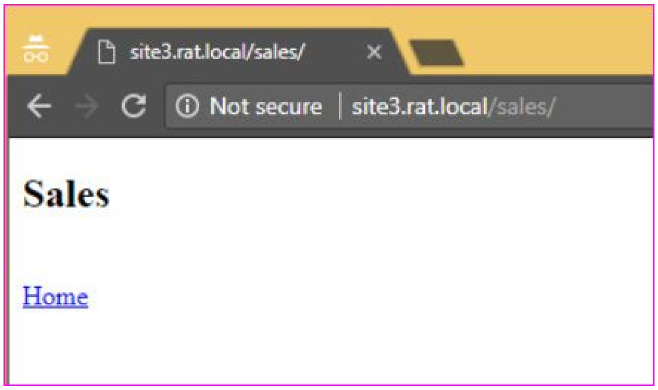
Sign in: Accounting
Sign in: Sales
Sign in: Marketing

Authentication required

http://site3.rat.local
Your connection to this site is not private

Username: sales4
Password: •••••••••••••

Proof I can access sales via windows authentication.



Sales

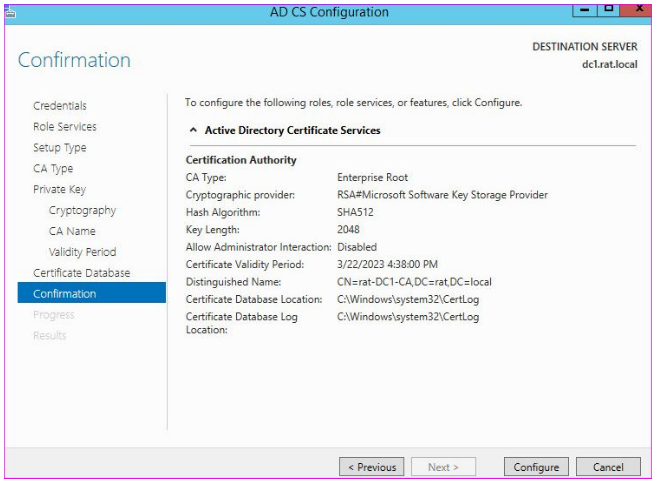
Home

Now we have our virtual Directories and can begin with site4's SSL.

IIS Site4 Configuration

First put a directory under the **Inetpub** directory called **admins**.
Then go to server manager and download/configure the role **Active Directory Certificate Services** with **Certificate Authority**, **Certificate Enrollment Policy Web Service**, **Certificate Enrollment Web Service**, **Certificate Authority Web Enrollment**.

A Summary of the Configuration for **Certificate Authority**



Confirmation

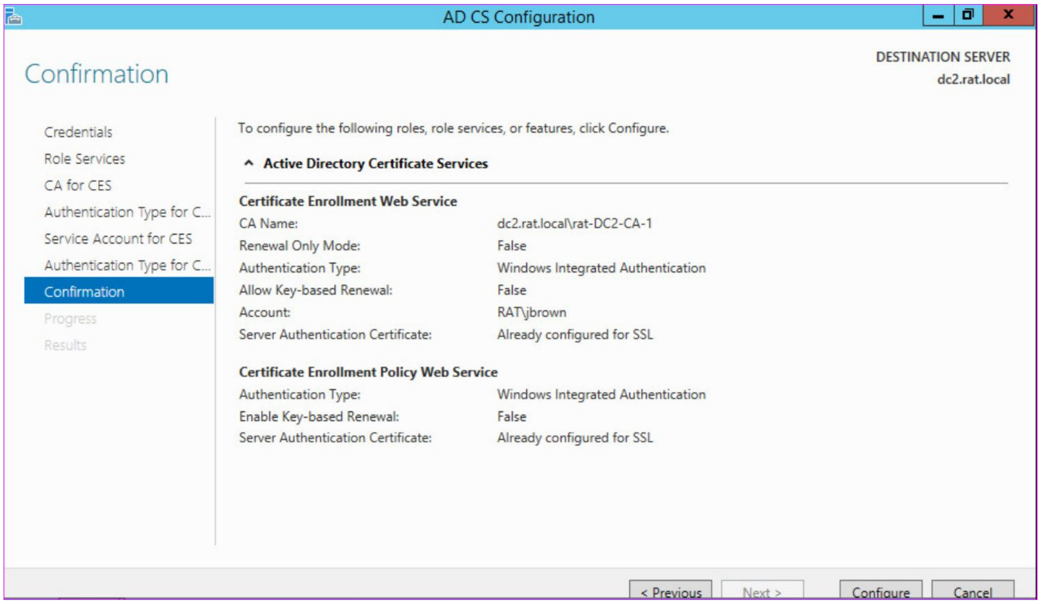
DESTINATION SERVER
dc1.rat.local

To configure the following roles, role services, or features, click Configure.

Active Directory Certificate Services

Certification Authority
CA Type: Enterprise Root
Cryptographic provider: RSA#Microsoft Software Key Storage Provider
Hash Algorithm: SHA512
Key Length: 2048
Allow Administrator Interaction: Disabled
Certificate Validity Period: 3/22/2023 4:38:00 PM
Distinguished Name: CN=rat-DC1-CA,DC=rat,DC=local
Certificate Database Location: C:\Windows\system32\CertLog
Certificate Database Log Location: C:\Windows\system32\CertLog

A Summary of the Configuration for **Certificate Enrollment Web Service**, and **Certificate Enrollment Policy Web Service**.



Confirmation

DESTINATION SERVER
dc2.rat.local

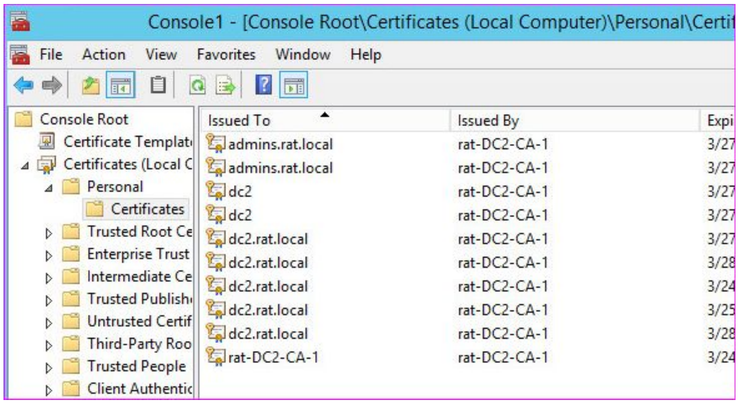
To configure the following roles, role services, or features, click Configure.

Active Directory Certificate Services

Certificate Enrollment Web Service
CA Name: dc2.rat.local\rat-DC2-CA-1
Renewal Only Mode: False
Authentication Type: Windows Integrated Authentication
Allow Key-based Renewal: False
Account: RAT\jbrown
Server Authentication Certificate: Already configured for SSL

Certificate Enrollment Policy Web Service
Authentication Type: Windows Integrated Authentication
Enable Key-based Renewal: False
Server Authentication Certificate: Already configured for SSL

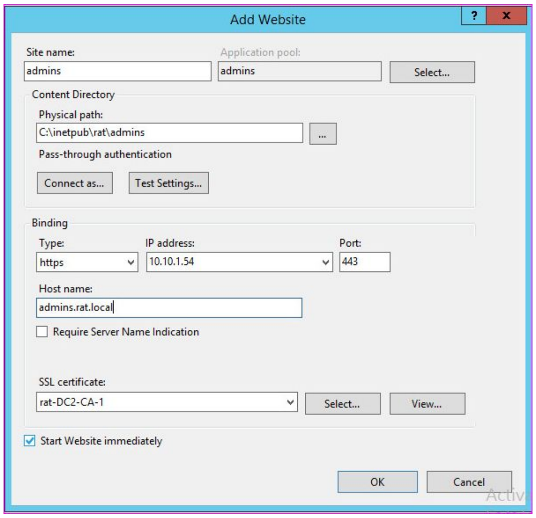
Right click **Windows** click **run** type **mmc** and click **ok**, go to **File** > **Add/Remove Snap-in** click on **Certificates**, then **Add >**, click **Ok**. When prompt select **Computer account**, select **Local computer** and click **Finish**. Once inside go to **Certificates** > **Personal** > **right click Certificates** click **All Tasks** > **Request New Certificate**. Once inside the **Certificate Enrollment** wizard click **Next**. Choose **Active Directory Enrollment Policy** click **Next**, choose **Domain Controller Authentication**, and click **Enroll**.



Console1 - [Console Root\Certificates (Local Computer)\Personal\Certi

Issued To	Issued By	Expi
admins.rat.local	rat-DC2-CA-1	3/27
admins.rat.local	rat-DC2-CA-1	3/27
dc2	rat-DC2-CA-1	3/27
dc2	rat-DC2-CA-1	3/27
dc2.rat.local	rat-DC2-CA-1	3/27
dc2.rat.local	rat-DC2-CA-1	3/28
dc2.rat.local	rat-DC2-CA-1	3/24
dc2.rat.local	rat-DC2-CA-1	3/25
dc2.rat.local	rat-DC2-CA-1	3/28
rat-DC2-CA-1	rat-DC2-CA-1	3/24

Now we can create the actual site, inside IIS.
give the site the name **admins** find the physical path click **Ok**, change **Type** to **https** select an **IP address** in the drop down box, and give a hostname of **admins.domain.local**. And select the certificate you just created. Click **Ok.**



Add Website

Site name: admins

Application pool: admins

Content Directory

Physical path: C:\inetpub\rat\admins

Pass-through authentication

Binding

Type: https

IP address: 10.10.1.54

Port: 443

Host name: admins.rat.local

☐ Require Server Name Indication

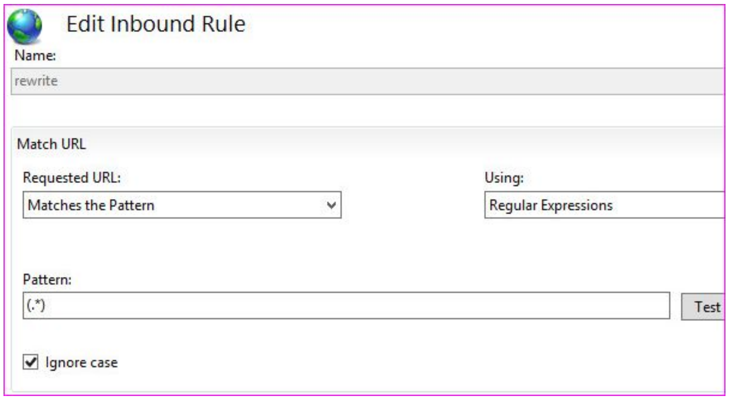
SSL certificate: rat-DC2-CA-1

☑ Start Website immediately

Right click on the site you just created and click **edit bindings**, click **Add** make sure it is **http**, select the same **IP** as the https, and give it the same host name “**admins.rat.local**”. Click **Ok**.

Next click on the site **admins** then go to **Authentication** disable **Anonymous Authentication** and enable **Windows Authentication**. Now we need to create a rule to allow only administrators to this site. Go to **Authorization Rules**, click **Add allow rule**, select **Specified roles or user groups** type in **administrators** then click **Ok**.

Next we need to install the module for rewriting http to https, go to the IIS official site and download **URL Rewrite**.
(https://www.iis.net/downloads/microsoft/url-rewrite) Once you have downloaded the module close and reopen IIS.
Now click on **admins** and go to **URL Rewrite** click **Add Rule** and select **Blank rule**(inbound). Give the **Inbound Rule** a name, under **Match URL** use the following settings:



Edit Inbound Rule

Name: rewrite

Match URL

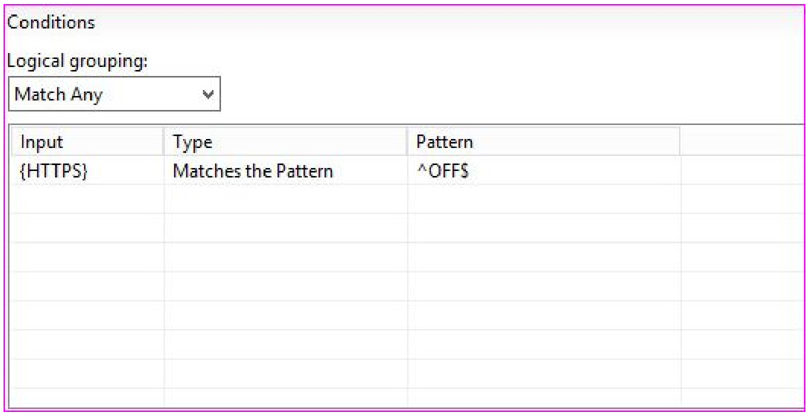
Requested URL: Matches the Pattern

Using: Regular Expressions

Pattern: (.*)

☑ Ignore case

Next under Match URL go to **Conditions** click **Add**, inside **Condition input** type {HTTPS} for **Pattern** type ^OFF$ and click **Ok**.

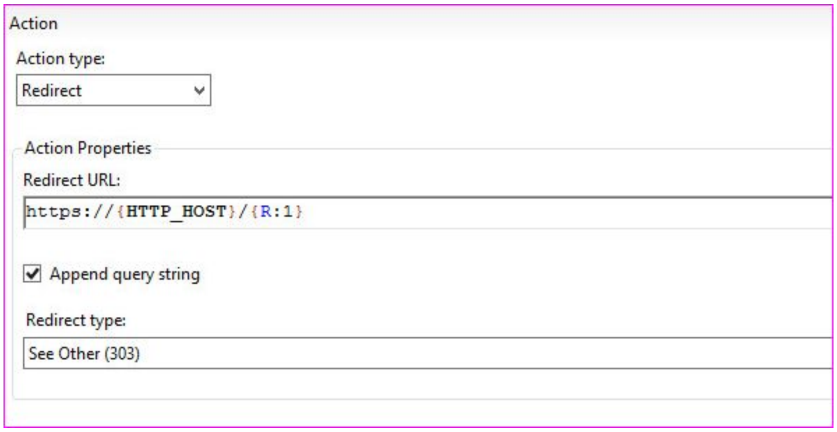


Conditions

Logical grouping: Match Any

Input	Type	Pattern
{HTTPS}	Matches the Pattern	^OFF$

Next under **Condition Input** go to **Action** change the **Action type** to **Redirect**, under **Redirect URL** type https://{HTTP_HOST}/{R:1}, and under **Redirect type** select **See Other (303)** once finished at the top right of the page hit **Apply**.



Action

Action type: Redirect

Action Properties

Redirect URL:

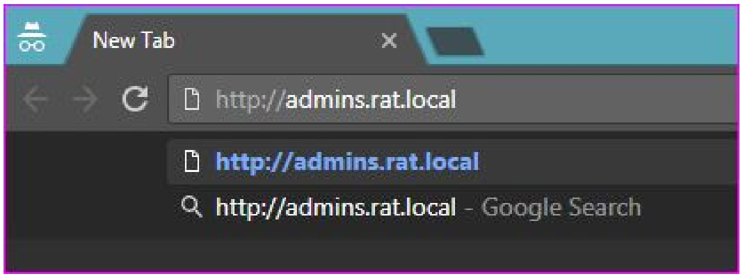
```
https://{HTTP_HOST}/{R:1}
```

☑ Append query string

Redirect type: See Other (303)

Now once you type http://admins.rat.local in a client's browser it will redirect to https://admins.rat.local and prompt for a password of an administrator, it will give no errors going into the site but has an error for SSL saying it isn't secure while in the site, I did try remaking the AD CS and giving it SHA512 but it still had the error.

Testing redirection (typing http://admins.rat.local and getting redirected to https://admins.rat.local):

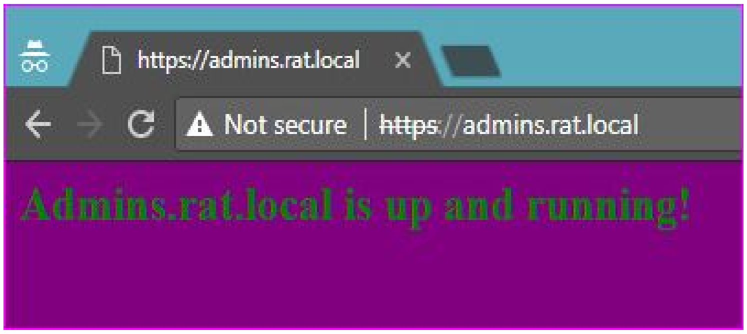


http://admins.rat.local

http://admins.rat.local

http://admins.rat.local - Google Search

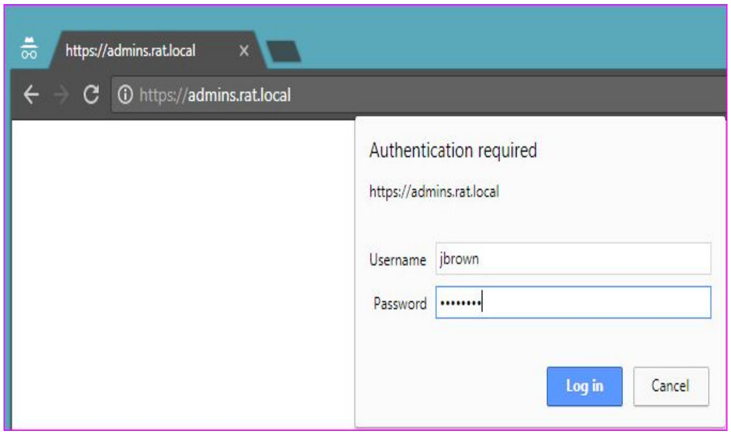
It goes right to https://admins.rat.local



~~https~~://admins.rat.local

Admins.rat.local is up and running!

Here is an example of the authentication, which allows only user in the administrators role.



Authentication required

https://admins.rat.local

Username: jbrown

Password: ••••••••

SSL encryption finished.

Part 2 - Network and Server monitoring

The first, and only monitoring software I tested is called PRTG by the company paessler (Download/information: https://www.paessler.com/prtg/download).

A few monitoring features PRTG has working with no initial set up other than DNS password and login to their cloud based website are:

- SNMP
- WMI
- SSH
- FLOWS and Packet Sniffing
- HTTP requests
- Ping
- SQL
- Disk Usage
- Memory Usage
- UpTime

And many more features without set up right out of the box.

If PRTG spots an error it will send you an email(the email you specify when setting it up) with all the verbose monitoring and error information on whatever's having a problem.

Costs

PRTG has a great selection of business License prices. PRTGs' lowest prices are starting at $1,600.00 for 12 months per 500 users(12 months is the shortest available license option). The most expensive License option is the PRTG XL5 36 Months, this costs $85,500.00. For more information on PRTG pricing go to: https://www.tweakservers.com/prtg-price-list/

PROS & CONS

Pros

- Very fast install, and works right on start up.
- The GUI is very straightforward to navigate through.
- When clicking on an attribute it shows a great deal of monitoring information.
- Easy to add additional sensors, and the sensors are free up to the 100th.
- Finds the even the slightest warnings, errors, and it emails them directly to you with monitoring information.

Cons

- On initial start up when discovering nearby instances/services takes quite a while.
- The desktop client is not up to par with the web client(lots of bugs).
- When first getting into PRTG in web, the interface seems overwhelming.
- It can Spams unnecessary error emails, after having PRTG set up for less than 5 minutes I've gotten over 10 emails.

Overall if payment was a non-factor especially for a startup businesses, I would recommend PRTG as a windows monitoring service. Some monitoring services take hours just to add an instance, PRTG adds everything it can find to monitor almost instantly, or as soon as its discovered. It works right away and works well, definitely a must have or at the very least a must try monitoring service.

Summary

Overall this project was fairly straight forward with only a few bumps in the road, like setting up AD CS and figuring out redirection; other than that everything else was very simple to set up and configure. This project was a great learning experience on hosting web servers and server monitoring from windows side of things.

References

- https://www.youtube.com/watch?v=O26CTdIOGUE
- https://www.youtube.com/watch?v=tNAdv1EPj-I
- https://www.youtube.com/watch?v=eU-VVggY_Vs
- https://www.youtube.com/watch?v=K33fwXnNfAk
- https://www.getapp.com/security-software/a/paessler/reviews/
- https://www.globalsign.com/en/blog/top-ssl-certificate-errors-and-solutions/