

Running UFM Server Software

Table of contents

Running UFM Server Software in Management Mode
Running UFM Software in High Availability Mode
HTTP/HTTPS Configuration
UFM Internal Web Server Configuration
User Authentication
UFM Authentication Server
Configurations of the UFM Authentication Server
Azure AD Authentication
Register UFM in Azure AD Portal
Enable Azure Authentication From UFM
Azure Authentication Login Page
Kerberos Authentication
Setting Up Kerberos Server Machine
Setting Up Kerberos Client Machine
Licensing
Showing UFM Processes Status

Before running UFM:

- Perform Initial Configuration
- Ensure that all ports used by the UFM server for internal and external communication are open and available. For the list of ports, see <u>Used Ports</u>.

You can run the UFM server software in the following modes:

- •
- <u>Running UFM Server Software in Management Mode</u>
- Running UFM Software in High Availability Mode
- Running UFM in High Availability with failover to an external SM

j) Note

In Management or High Availability mode, ensure that all Subnet Managers in the fabric are disabled *before* running UFM. Any remaining active Subnet Managers will prevent UFM from running.

Running UFM Server Software in Management Mode

After installing, run the UFM Server by invoking:

systemctl start ufm-enterprise.service



/etc/init.d/ufmd - Available for backward compatibility.

Log files are located under /opt/ufm/files/log (the links to log files are in /opt/ufm/log).

Running UFM Software in High Availability Mode

On the Master server, run the UFM Server by invoking:

ufm_ha_cluster start

You can specify additional command options for the ufmha service.

ufm_ha_cluster Command Options

Command	Description
start	Starts UFM HA cluster.
stop	Stops UFM HA cluster.
failover	Initiates failover (change mastership from local server to remote server).
takeover	Initiates takeover (change mastership from remote server to local server).
status	Shows current HA cluster status.
cleanup	Cleans the HA configurations on this node.
help	Displays help text.

HTTP/HTTPS Configuration

By default, UFM is configured to work with the secured HTTPS protocol.

After installation, the user can change the the Web Server configuration to communicate in secure (HTTPS) or non-secure (HTTP) protocol.

For changing the communication protocol, use the following parameter under the [Server] section in the gv.cfg file:

• ws_protocol = https

Changes will take effect after restarting UFM.

UFM Internal Web Server Configuration

UFM uses Apache as the main Web Server for client external access. The UFM uses an internal web server process to where the Apache forwards the incoming requests.

By default, the internal web server listens to the local host interface (127.0.0.1) on port 8000.

For changing the listening local interface or port, use the following parameters under the [Server] section in the gv.cfg file:

- rest_interface = 127.0.0.1
- rest_port = 8000

Changes will take effect after restarting UFM.

User Authentication

UFM User Authentication is based on standard Apache User Authentication. Each Web Service client application must authenticate against the UFM server to gain access to the system.

The UFM software comes with one predefined user:

- Username: admin
- Password: 123456

You can add, delete, or update users via User Management Tab.

UFM Authentication Server

The UFM Authentication Server, a centralized HTTP server, is responsible for managing various authentication methods supported by UFM.

Configurations of the UFM Authentication Server

The UFM Authentication Server is designed to be configurable and is initially turned off by default. This means that existing authentication methods are managed either by the native Apache functionality (such as Basic, Session, and Client Certificate authentication) or at the UFM level (including Token-Based authentication and Proxy Authentication).

Enabling the UFM Authentication Server provides a centralized service that oversees all supported authentication methods within a single service, consolidating them under a unified authentication API.

Apache utilizes the authentication server's APIs to determine a user's authentication status.

To enable the UFM Authentication Server, refer to Enabling UFM Authentication Server.

All activities of the UFM Authentication Server are logged in the authentication_service.log file, located at /opt/ufm/files/log.

Azure AD Authentication

Microsoft Azure Authentication is a service provided by Microsoft Azure, the cloud computing platform of Microsoft. It is designed to provide secure access control and authentication for applications and services hosted on Azure.

UFM supports Authentication using Azure Active Directory, and to do so, you need to follow the following steps:

Register UFM in Azure AD Portal

To log in via Azure, UFM must be registered in the Azure portal using the following steps:

- 1. Log in to <u>Azure Portal</u>, then click "**Azure Active Directory"** in the side menu.
- 2. If you have access to more than one tenant, select your account in the upper right. Set your session to the Azure AD tenant you wish to use.
- 3. Under "**Manage"** in the side menu, click App Registrations > New Registration.

Microsoft Azure		$\mathcal P$ Search resources, services, and docs (G+/)
Home > NVIDIA Corporation		
NVIDIA Corporation	n App registrations 🛷 …	
Overview	+ New registration 🕀 Endpoints 🤌 T	roubleshooting 💍 Refresh 🞍 Download 🐼 Preview feat
 Preview features Diagnose and solve problems 	Starting June 30th, 2020 we will no longer upgraded to Microsoft Authentication Libra	add any new features to Azure Active Directory Authentication Library (, ary (MSAL) and Microsoft Graph. <u>Learn more</u>
Manage		
🚨 Users	All applications Owned applications	Deleted applications
🎥 Groups	Start typing a display name or application	n (client) ID to filter these r
External Identities		
a, Roles and administrators	1 applications found	
Administrative units		
🚸 Delegated admin partners	OF OFMAPP	
Enterprise applications		
Devices App registrations		
Identity Governance		
Application proxy		

- 4. Provide the application details:
 - 1. **Name**: Enter a descriptive name.
 - 2. **Supported account types**: Account types that are allowed to login and use the registered application.
 - 3. **Redirect URL**: select the app type **Web**, and Add the following redirect URL https:///auth/login

Home > NVIDIA Corporation | App registrations >

Register an application

* Name

The user-facing display name for this application (this can be changed later).

UFM_APP			~
Supported accou	nt types		
Who can use this app	lication or access	his API?	
Accounts in this	organizational dire	ctory only (NVIDIA Corporation only - Single tenant)	
Accounts in any	organizational dire	ctory (Any Azure AD directory - Multitenant)	
 Accounts in any 	organizational dire	ctory (Any Azure AD directory - Multitenant) and personal Microsoft ac	counts (e.g. Skype, Xbox)
Personal Microso	oft accounts only		
Help me choose			
Redirect URI (opti We'll return the authe changed later, but a v	ional) entication response value is required fo	to this URI after successfully authenticating the user. Providing this nor r most authentication scenarios.	w is optional and it can be
Web	\sim	https://10.209.36.68/auth/login	~
Register an app you'r	e working on here	Integrate gallery apps and other apps from outside your organization I	by adding from Enterprise application
By proceeding, you a	gree to the Micros	oft Platform Policies 🔄	
Popistor			

Then, click **Register**. The app's **Overview** page opens.

5. Under **Manage** in the side menu, click **Certificates & Secrets** > New client secret.

Add a client secret		×
Description	UFM_APP_sec	
Expires	Recommended: 180 days (6 months)	\sim

Provide a description for the client secret and set an expiration time, then click "**Add**."

6. Copy the client secret key value which will be needed to configure the UFM with Azure AD (Please note that the value of the generated secret will be hidden and will not be able to be copied/read after you leave the page.

Home > NVIDIA Corporation | App registrations > UFM-APP 🔣 UFM-APP | App roles 👒 … P Search K + Create app role R Got feedback? Cven/ex Quickstert Oct a second to give us some feedback? → 💉 Integration assistant App roles Manage App roles are outom roles to assign permissions to users or apps. The application defines and publishes the app roles and interprets them as permissions during authorization. Branding & properties Authentication How do I assign App roles Certificates & secrets Display name Description Allowed member types Value ID. State Tokan configuration No app roles have been added. API permissions Expose an API App roles Owners 🕹 Roles and administrators Manifest Support + Troubleshooting P Troubleshooting New support request

Under "**Manage"** in the side menu, click App roles > Create app role.

7. Provide the role details. Please note that the role value must be a valid UFM role; otherwise, the login will fail.

Create app role	×
Display name * ()	
System Admin	~
Allowed member types * ()	
Both (Users/Groups + Applications)	
Value * 🛈	
System_Admin	~
Description * ①	
System_Admin	
Do you want to enable this app role? ()	

8. Assign the created role to the user. Follow the below steps:



Properties

Name ① Copy to clipboard	
UFM-APP	
Application ID ①	
0d5e6cda-9144-47a2-b685 🗈	
Object ID ①	
dd2a68d5-a3e0-45e3-9c1c 🗈	
Getting Started	
3	
1. Assign users and groups	2. Provision User Accounts
Provide specific users and groups access to the applications	You'll need to create user accounts in the application
Assign users and groups	Learn more
 Self service Enable users to request access to the application using their Azure AD 	
credentials Get started	
+ Add user/group ⁴ Edit assignment III Remove & Update	credentials ≡≡ Columns 🖗 Got feedback?
The application will not appear for assigned users within My Apps. Set 'visib	le to users?' to yes in properties to enable this. \rightarrow
Assign users and groups to app-roles for your application here. To create new	v app-roles for this application, use the application registration.
Display Name Object Type	Role assigned
No application assignments found	

Home > UFM-APP | App roles > UFM-APP | Users and groups >

Users and groups 1 user selected.	
1 user selected.	
Select a role *	
System_Admin	

9. Click on "**Overview**" in the side menu to view the application information, such as tenant ID, client ID, and other details.

Enable Azure Authentication From UFM

Azure authentication is disabled by default. To enable it, please refer to <u>Enabling Azure</u> <u>AD Authentication</u>.

Azure Authentication Login Page

After enabling and configuring Azure AD authentication, an additional button will appear on the primary UFM login page labeled 'Sign In with Microsoft,' which will leads to the main Microsoft sign-in page:

	UFM
Username	
Password	
Login	
OR	
Sign in with Microsoft	

Kerberos Authentication

Kerberos is a network authentication protocol designed to provide strong authentication for client-server applications by using secret-key cryptography.

The Kerberos protocol works on the basis of tickets, it helps ensure that communication between various entities in a network is secure. It uses symmetric-key cryptography, which means both the client and servers share secret keys for encrypting and decrypting communication.

To enable Kerberos Authentication, refer to Enabling Kerberos Authentication.

Setting Up Kerberos Server Machine

To set up a system as a Kerberos server, perform the following:

1. Install the required packages:

#Redhatsudo yum install krb5-libs krb5-server# Ubuntusudo apt-get install krb5-kdc krb5-admin-server

2. Edit the Kerberos configuration file '/etc/krb5.conf' to reflect your realm, domain and other settings:

```
[libdefaults]
  default_realm = YOUR-REALM
[realms]
  YOUR-REALM = {
    kdc = your-kdc-server
    admin_server = your-admin-server
  }
[domain_realm]
  your-domain = YOUR-REALM
  your-domain = YOUR-REALM
```

3. Use the kdb5_util command to create the Kerberos database:

kdb5_util create -r YOUR-REALM -s

4. Add administrative principals:

Kadmin.local addprinc -randkey HTTP/YOUR-HOST-NAME@YOUR-REALM

5. Start KDC and Kadmin services:

sudo systemctl start krb5kdc kadmin sudo systemctl enable krb5kdc kadmin

6. Generate a keytab file. The keytab file contains the secret key for a principal and is used to authenticate the service.

kadmin.local ktadd -k /path/to/your-keytab-file HTTP/YOUR-HOST-NAME@YOUR-REALM

Replace /path/to/your-keytab-file with the actual path where you want to store the keytab file.

Setting Up Kerberos Client Machine

Follow the below steps to set up a system as a Kerberos client.

1. Install the required packages. When installing the UFM, the following packages will be installed as dependencies:

#Redhatkrb5-libs krb5-workstation mod_auth_gssapi# Ubuntukrb5-config krb5-user libapache2-mod-auth-gssapi

2. Configure the /etc/krb5.conf file to reflect your realm, domain, local names map and other settings:

```
[libdefaults]
default_realm = YOUR-REALM
[realms]
YOUR-REALM = {
kdc = your-kdc-server
admin_server = your-admin-server
auth_to_local_names = {
your-principle-name = your-local-user
}
}
[domain_realm]
your-domain = YOUR-REALM
your-domain = YOUR-REALM
```

3. Copy the keytab file from the Kerberos server to the machine where your service runs (the client). It is important to ensure that it is kept confidential.

Please ensure that the keytab file exists and that Apache has the necessary read permissions to access the keytab file; otherwise, Kerberos authentication will not function properly.

4. Obtain a Kerberos ticket-granting ticket (TGT):

kinit -k -t /path/to/your-keytab-file HTTP/YOUR-HOST-NAME@YOUR-REALM

- 5. Enable Kerberos Authentication from UFM. Kerberos authentication is disabled by default. To enable it, please refer to <u>Enabling Kerberos Authentication</u>.
- 6. Test the Kerberos Authentication. You can use curl to test whether the user can authenticate to UFM REST APIs using Kerberos.

curl --negotiate -i -u : -k 'https://ufmc-eos01/ufmRestKrb/app/tokens'

Licensing

UFM license is subscription-based featuring the following subscription options:

- 1-year subscription
- 3-year subscription
- 5-year subscription
- Evaluation 30-day trial license



UFM will continue to support old license types, but they are no longer available to obtain.

2 months before the expiration of your subscription license, UFM will warn you that your license will expire soon. After the subscription expires, UFM will continue to work with the expired license for two months beyond its expiration.

During this extra two-month period, UFM will generate a critical alarm indicating that the UFM license has expired and that you need to renew your subscription. Failing to do so within that 2-month period activates UFM Limited Mode. Limited mode blocks all REST APIs and access to the UFM web UI.

UFM enables functionality based on the license that was purchased and installed. This license determines the functionality and the maximum allowed number of nodes in the fabric.

To renew your UFM subscription, purchase a new license and install the new license file by downloading the license file to a temp directory on the UFM master server and then copying the license file to /opt/ufm/files/licenses/ directory.

j Note

UFM may not detect new license files if downloaded directly to /opt/ufm/files/licenses. If UFM does not detect the new license file, a UFM restart may be required.

If several licenses are installed on the server (more than one license file exists under /opt/ufm/files/licenses/), UFM uses only the strongest license and takes into consideration the expiration date, and the managed device limits on it, regardless of any other licenses that may exist on the server.

Showing UFM Processes Status

This functionality allows users to view the current status of main processes handled by the UFM.

- To view the main UFM processes, run the script show_ufm_status.sh under the /opt/ufm/scripts.Example: /opt/ufm/scripts/show_ufm_status.sh
- To view the UFM main and child processes, run the script show_ufm_status.sh with -e (extended_processes).

Example: /opt/ufm/scripts/show_ufm_status.sh -e

[root@r-ufm77 gv	/vm_github]# /opt/ufm/scripts/show_ufm_status.sh
	UFM Main Processes
ModelMain	Process is : [Running]
Opensm	Process is : [Running]
SHARP	Process is : [Running]
Unhealthy Ports	Process is : [Running]
Daily Report	Process is : [Running]
UFM Health	Process is : [Running]
UFM Telemetry	Process is : [Running]
[root@r-ufm77_ov	vm_oithubl#_/oot/ufm/scripts/show_ufm_status_she
(10000) 01011 910	
	UFM Main Processes
ModelMain	Process is : [Running]
Opensm	Process is : [Running]
SHARP	Process is : [Running]
Unhealthy Ports	Process is : [Running]
Daily Report	Process is : [Running]
UFM Health	Process is : [Running]
UFM Telemetry	Process is : [Running]
	UFM ModelMain Child Processes
au a 2 /	
SMCLientConsumer	Process is : [Running]
SMirapHandler	Process is : [Kunning]
SysintoJsonAgent	Process 1s : [Running]
Telemetry Agent	Process is : [Running]
recemetry History	y process is : [wonding]
	© Copyright 2024, NVIDIA. PDF Generated on 08/14/2024