Global File Cache documentation

Global File Cache

NetApp
April 04, 2022

This PDF was generated from https://docs.netapp.com/us-en/cloud-manager-file-cache/index.html on April 04, 2022. Always check docs.netapp.com for the latest.

Table of Contents

Global File Cache documentation . . . 1
Release notes . . . 2
- What's new with Global File Cache . . . 2
- Fixed issues in Global File Cache . . . 2

Get started . . . 4
- Learn about Global File Cache . . . 4
- Before you begin to deploy Global File Cache . . . 7
- Getting started . . . 11
- Before you begin to deploy Global File Cache Edge instances . . . 23
- Deploy Global File Cache Edge instances . . . 29

Use Global File Cache . . . 33
- End-user training . . . 33
- Additional information . . . 33

Knowledge and support . . . 34
- Register for support . . . 34
- Get help . . . 35

Legal notices . . . 36
- Copyright . . . 36
- Trademarks . . . 36
- Patents . . . 36
- Privacy policy . . . 36
- Open source . . . 36

Global File Cache documentation

Release notes

What's new with Global File Cache

Learn what's new in Global File Cache.

17 December 2021 (version 1.2.0)

The OpenSSL module has been upgraded to version 1.1.1l.

This is the latest version and it is more secure. This module is used for secure communication between GFC Edge and GFC Core.

The logging infrastructure has been enhanced.

9 June 2021 (version 1.1.0)

The "Edge Synchronization" feature has been added.

This feature keeps multiple Edges at a remote office in sync and the data is always cached/warm. When a file is flushed/fetched at one Edge, then the same file on all Edges participating in Edge Sync is updated and cached. See section 8.4 in the NetApp Global File Cache User Guide for details.

The OpenSSL module has been upgraded to version 1.1.1k.

This is the latest version and it is more secure. This module is used for secure communication between GFC Edge and GFC Core.

Updated License Registration Page.

The GFC License Registration Page now displays the number of licenses when activated through a NetApp subscription.

21 March 2021 (version 1.0.3)

Software installer updates to automatically exclude GFC process from Windows Defender.

The Global File Cache software installer now excludes all GFC processes from Windows Defender software on-demand scanning.

A new Policy Configuration tab has been added to the Configuration Console.

This configuration tab enables you to add pre-population jobs from the GFC Core.

Enhanced the software to use less memory while increasing performance and stability.

Fixed issues in Global File Cache

See what issues have been fixed in Global File Cache.

17 December 2021 (version 1.2.0)

- The Configuration UI (Optimus) is enhanced to validate the date field entries while adding pre-population jobs.
- Pre-population is enhanced to monitor cache utilization and will skip populating if cache usage reaches close to cache cleaner parameters.
- Removed the hard dependency of the License Management Server (LMS) Service running locally with Policy configuration.
- The GFC Kernel driver is enhanced to avoid a crash in the SMB Server service in Windows Server 2016/2019.
- Fixed an exception in the LMS Service.
- Service Start types for LMS, LMC, and TappN Services are changed from 'Automatic Delayed' to 'Automatic'.

9 June 2021 (version 1.1.0)

- The Configuration UI now displays the Edge hostname correctly in the Edit Pre-population page.
- An issue in parsing the json response from the NetApp License subscription server during license registration is fixed.
- Pre-population (TappN) logs are enhanced to log the file transfer status of all the files.

7 April 2021 (version 1.0.4)

- A QoS issue has been fixed where QoS parameters were applied to *all* users instead of just the user who surpassed the limits.
- NSS credentials are now validated before being applied to the licensing system.
- Race conditions between the GFC software and certain antivirus software have been fixed.
- A crash no longer occurs when a locking hierarchy is violated during drop lease operations.

21 March 2021 (version 1.0.3)

- The NetApp license registration and GFC subscription-based registration is only allowed by the cloud-based License Management Server (LMS). The on-premises LMS should use legacy licensing.
- The Configuration UI now adds jobs in pre-population when the License Manager Client Service (LMC) uses hostnames instead of IP address for the LMS during configuration.

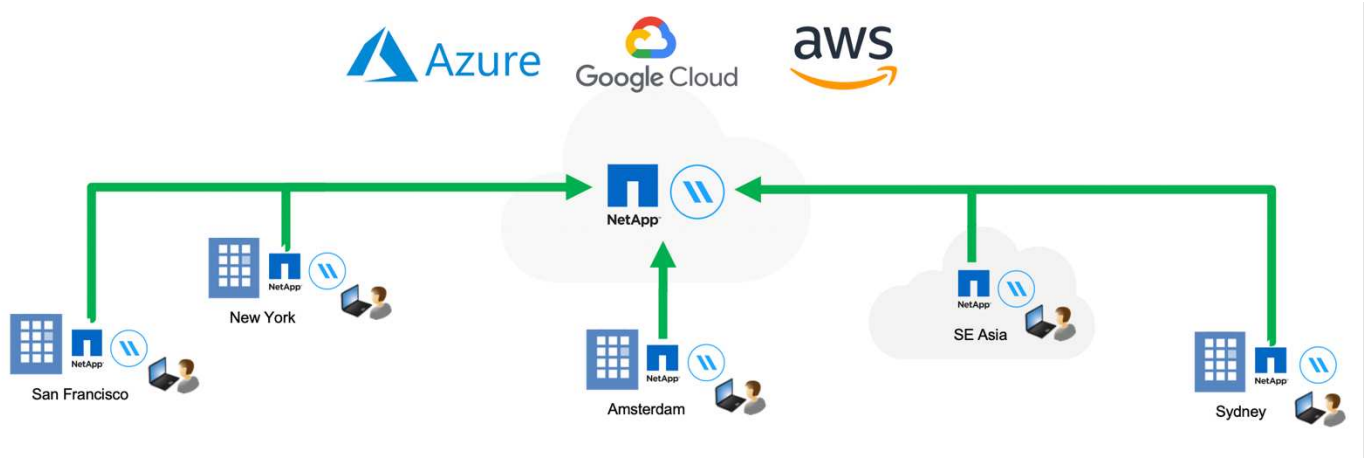
Get started

Learn about Global File Cache

NetApp Global File Cache enables you to consolidate silos of distributed file servers into one cohesive global storage footprint in the public cloud. This creates a globally accessible file system in the cloud that all remote locations can use as if they were local.

Overview

Implementing Global File Cache results in a single, centralized storage footprint, versus a distributed storage architecture that requires local data management, backup, security management, storage, and infrastructure footprint in each location.



Features

Global File Cache enables the following features:

- Consolidate and centralize your data into the public cloud and leverage the scalability and performance from enterprise-grade storage solutions
- Create a single set of data for users globally and leverage intelligent file caching to improve global data access, collaboration, and performance
- Rely on a self-sustaining, self-managing cache, and eliminate full data copies and backups. Utilize local file caching for active data and cut storage costs
- Transparent access from branch locations through a global namespace with real time central file locking

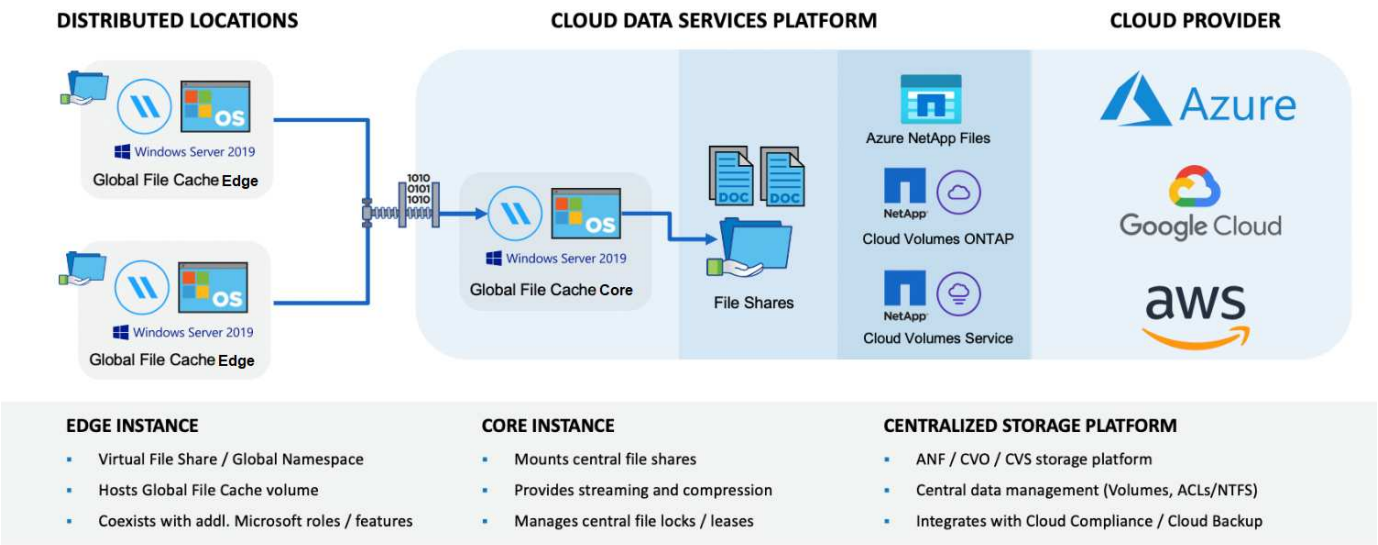
See more about Global File Cache features and use cases here.

Global File Cache components

Global File Cache consists of the following components:

- Global File Cache Management Server
- Global File Cache Core
- Global File Cache Edge (deployed in your remote locations)

The Global File Cache Core instance mounts to your corporate file shares hosted on your backend storage platform of choice (such as Cloud Volumes ONTAP, Cloud Volumes Service, and Azure NetApp Files) and creates the Global File Cache Fabric that provides the ability to centralize and consolidate unstructured data into a single set of data, whether it resides on one or multiple storage platforms in the public cloud.



Supported storage platforms

The supported storage platforms for Global File Cache differ depending on the deployment option you select.

Automated deployment options

Global File Cache is supported with the following types of working environments when deployed using Cloud Manager:

- Cloud Volumes ONTAP in Azure
- Cloud Volumes ONTAP in AWS

This configuration lets you deploy and manage the entire Global File Cache server-side deployment, including Global File Cache Management Server and Global File Cache Core, from within Cloud Manager.

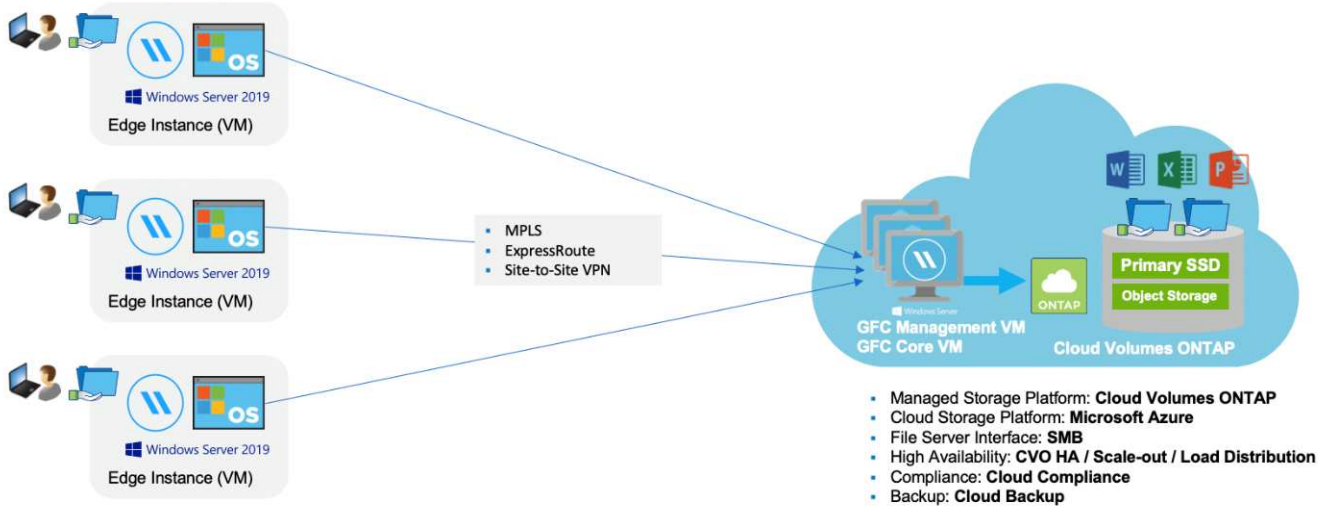
Manual deployment options

Global File Cache configurations are also supported with Cloud Volumes ONTAP, Cloud Volumes Service, Azure NetApp Files, and Amazon FSx for ONTAP systems installed on public cloud storage infrastructure. On-premises solutions are also available on NetApp AFF and FAS platforms. In these installations the Global File Cache server-side components must be configured and deployed manually, not using Cloud Manager.

See the NetApp Global File Cache User Guide for details.

How Global File Cache works

Global File Cache creates a software fabric that caches active data sets in remote offices globally. As a result, business users are guaranteed transparent data access and optimal performance on a global scale.



The topology referenced in this example is a hub and spoke model, whereby the network of remote offices/locations is accessing one common set of data in the cloud. The key points of this example are:

- Centralized data store:
  - Enterprise public cloud storage platform, such as Cloud Volumes ONTAP
- Global File Cache Fabric:
  - Extension of the central data store to the remote locations
  - Global File Cache Core instance, mounting to corporate file shares (SMB).
  - Global File Cache Edge instances running in each remote location.
  - Presents a virtual file share in each remote location that provides access to central data.
  - Hosts the Intelligent File Cache on a custom-sized NTFS volume (`D:\`).
- Network configuration:
  - Multiprotocol Label Switching (MPLS), ExpressRoute, or VPN connectivity
- Integration with customer's Active Directory domain services.
- DFS namespace for the use of a global namespace (recommended).

Cost

The cost to use Global File Cache depends on the type of installation you have chosen.

- All installations require that you deploy one or more volumes in the cloud (Cloud Volumes ONTAP, Cloud Volumes Service, or Azure NetApp Files). This results in charges from the selected cloud provider.
- All installations also require that you deploy two or more virtual machines (VMs) in the cloud. This results in charges from the selected cloud provider.
  - Global File Cache Management Server:

    In Azure, this runs on a D2s_V3 or equivalent (2 vCPU/8 GB RAM) VM with 127 GB premium SSD

    In AWS, this runs on a m4.large or equivalent (2 vCPU/8 GB RAM) instance with 127 GB general purpose SSD

- Global File Cache Core:

  In Azure, this runs on a D4s_V3 or equivalent (4 vCPU/16 GB RAM) VM with 127 GB premium SSD

  In AWS, this runs on a m4.xlarge or equivalent (4 vCPU/16 GB RAM) instance with 127 GB general purpose SSD

- When installed with Cloud Volumes ONTAP in Azure or AWS (the supported configurations deployed completely through Cloud Manager), there is a charge of $3,000 per site (for each Global File Cache Edge instance), per year.
- When installed using the manual deployment options the pricing is different. To see a high-level estimate of costs, see Calculate Your Savings Potential or consult your Global File Cache Solutions Engineer to discuss the best options for your enterprise deployment.

Licensing

Global File Cache includes a software-based License Management Server (LMS), which allows you to consolidate your license management and deploy licenses to all Core and Edge instances using an automated mechanism.

When you deploy your first Core instance in the datacenter or cloud, you can choose to designate that instance as the LMS for your organization. This LMS instance is configured once, connects to the subscription service (over HTTPS) and validates your subscription using the customer ID provided by our support/operations department upon enablement of the subscription. After you have made this designation, you associate your Edge instances with the LMS by providing your customer ID and the IP address of the LMS instance.

When you purchase additional Edge licenses or renew your subscription, our support/operations department updates the license details, for example, the number of sites or subscription end date. After the LMS queries the subscription service, the license details are automatically updated on the LMS instance and will apply to your GFC Core and Edge instances.

See the NetApp Global File Cache User Guide for additional details about licensing.

Limitations

The version of Global File Cache supported within Cloud Manager requires that the backend storage platform used as your central storage must be a working environment where you have deployed a Cloud Volumes ONTAP single node or HA pair in Azure or AWS.

Other storage platforms and other cloud providers are not supported at this time using Cloud Manager, but can be deployed using legacy deployment procedures.

These other configurations, for example, Global File Cache using Cloud Volumes ONTAP or Cloud Volumes Service on Microsoft Azure, Google Cloud, or AWS continue to be supported using the legacy procedures. See Global File Cache overview and onboarding for details.

Before you begin to deploy Global File Cache

There are many requirements you need to be aware of before you begin to deploy Global File Cache in the cloud and in your remote offices.

Global File Cache Core design considerations

Depending on your requirements, you may need to deploy one or multiple Global File Cache Core instances to create the Global File Cache Fabric. The Core instance is designed to act as a traffic cop between your distributed Global File Cache Edge instances and the data center file server resources, for example, file shares, folders, and files.

When you are designing your Global File Cache deployment you need to determine what's right for your environment in terms of scale, availability of resources, and in terms of redundancy. Global File Cache Core can be deployed in the following ways:

- GFC Core stand-alone instance
- GFC Core Load Distributed design (Cold Standby)

See Sizing guidelines to understand the maximum number of Edge instances and total users that each configuration can support:

Consult your Global File Cache Solutions Engineer to discuss the best options for your enterprise deployment.

Sizing guidelines

There are a few sizing guideline ratios that you need to keep in mind when configuring the initial system. You should revisit these ratios after some usage history has accumulated to make sure you are using the system optimally. These include:

- Global File Cache Edges/Core ratio
- Distributed users/Global File Cache Edge ratio
- Distributed users/Global File Cache Core ratio

Number of Edge Instances per Core Instance

Our guidelines recommend up to 10 Edge instances per Global File Cache Core instance, with a maximum of 20 Edges per Global File Cache Core instance. This is dependent to a significant degree upon the type and mean file size of the most common workload. In some cases, with more common workloads you can add more Edge instances per Core, but in these cases you should contact NetApp Support to correctly size the number of Edge and Core instances depending on the types and sizes of the file sets.

> You can leverage multiple Global File Cache Edge and Core instances simultaneously to scale out your infrastructure depending on the requirements.

Number of concurrent users per Edge instance

Global File Cache Edge handles the heavy lifting in terms of caching algorithms and file-level differencing. A single Global File Cache Edge instance can serve up to 400 users per dedicated physical Edge instance, and up to 200 users for dedicated virtual deployments. This is dependent to a significant degree upon the type and mean file size of the most common workload. For larger collaborative file types, guide towards 50% of the maximum users per Global File Cache Edge lower boundary (depending on physical or virtual deployment). For more common Office items with a mean file size <1MB, guide towards the 100% users per Global File Cache Edge upper boundary (depending on physical or virtual deployment).

Global File Cache Edge detects whether it is running on a virtual or physical instance and it will limit the number of SMB connections to the local virtual file share to the maximum of 200 or 400 concurrent connections.

Number of concurrent users per Core instance

The Global File Cache Core instance is extremely scalable, with a recommended concurrent user count of 3,000 users per Core. This is dependent to a significant degree upon the type and mean file size of the most common workload.

Consult your Global File Cache Solutions Engineer to discuss the best options for your enterprise deployment.

Prerequisites

The prerequisites described in this section are for the components installed in the cloud: the Global File Cache Management Server and the Global File Cache Core.

Global File Cache Edge prerequisites are described here.

Cloud Manager instance

When using Cloud Volumes ONTAP for Azure as your storage platform, ensure that Cloud Manager has permissions as shown in the latest Cloud Manager policy for Azure.

Newly created instances will have all the required permissions by default. If you deployed your instance prior to version 3.8.7 (August 3, 2020), then you will need to add these items.

```
"Microsoft.Resources/deployments/operationStatuses/read",
"Microsoft.Insights/Metrics/Read",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/virtualMachines/extensions/delete",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
```

Storage platform (volumes)

The back-end storage platform – in this case, your deployed Cloud Volumes ONTAP instance - should present SMB file shares. Any shares that will be exposed through Global File Cache must allow the Everyone group Full Control at the share level, while restricting permissions through NTFS permissions.

If you have not set up at least one SMB file share on the Cloud Volumes ONTAP instance, then you need to have the following information ready so you can configure this information during installation:

- Active Directory domain name, name server IP address, Active Directory admin credentials.
- The name and size of the volume you want to create, the name of the aggregate on which the volume will be created, and the share name.

We recommend that the volume is large enough to accommodate the total data set for the application along with the ability to scale accordingly as the data set grows. If you have multiple aggregates in the working environment, see Managing existing aggregates to determine which aggregate has the most available space for the new volume.

Global File Cache Management Server

This Global File Cache Management Server requires external access over HTTPS (TCP port 443) to connect to the cloud provider subscription service and to access these URLs:

- https://talonazuremicroservices.azurewebsites.net
- https://talonlicensing.table.core.windows.net

This port must be excluded from any WAN optimization devices or firewall restriction policies for the Global File Cache software to operate properly.

The Global File Cache Management Server also requires a unique (geographical) NetBIOS name for the instance (such as GFC-MS1).

> One Management Server can support multiple Global File Cache Core instances deployed in different working environments. When deployed from Cloud Manager, each working environment has its own separate backend storage and would not contain the same data.

Global File Cache Core

This Global File Cache Core listens on TCP port range 6618-6630. Depending on your firewall or Network Security Group (NSG) configuration you may need to explicitly allow access to these ports through Inbound Port Rules. Also, these ports must be excluded from any WAN optimization devices or firewall restriction policies for the Global File Cache software to operate properly.

The Global File Cache Core requirements are:

- A unique (geographical) NetBIOS name for the instance (such as GFC-CORE1)
- Active Directory domain name
  - Global File Cache instances should be joined to your Active Directory domain.
  - Global File Cache instances should be managed in a Global File Cache specific Organizational Unit (OU) and excluded from inherited company GPOs.
- Service account. The services on this Global File Cache Core run as a specific domain user account. This account, also known as the Service Account, must have the following privileges on each of the SMB servers that will be associated with the Global File Cache Core instance:
  - The provisioned Service Account must be a domain user.

    Depending on the level of restrictions and GPOs in the network environment, this account might require domain admin privileges.
  - It must have "Run as a Service" privileges.
  - The password should be set to "Never Expire".
  - The account option "User Must Change Password at Next Logon" should be DISABLED (unchecked).
  - It must be a member of the back-end file server Built-in Backup Operators group (this is automatically enabled when deployed through Cloud Manager).

License Management Server

- The Global File Cache License Management Server (LMS) should be configured on a Microsoft Windows Server 2016 Standard or Datacenter edition or Windows Server 2019 Standard or Datacenter edition, preferably on the Global File Cache Core instance in the datacenter or cloud.
- If you require a separate Global File Cache LMS instance, you need to install the latest Global File Cache software installation package on a pristine Microsoft Windows Server instance.
- The LMS instance needs to be able to connect to the subscription service (Azure Services / public internet) using HTTPS (TCP port 443).
- The Core and Edge instances need to connect to the LMS instance using HTTPS (TCP port 443).

Networking (External Access)

The Global File Cache LMS requires external access over HTTPS (TCP port 443) to the following URLs.

- If you are using GFC subscription-based licensing:
  - https://rest.zuora.com/v1/subscriptions/<subscription-no>
  - https://rest.zuora.com/oauth/token
- If you are using NetApp NSS-based licensing:
  - https://login.netapp.com
  - https://login.netapp.com/ms_oauth/oauth2/endpoints
  - https://login.netapp.com/ms_oauth/oauth2/endpoints/oauthservice/tokens
- If you are using NetApp legacy-based licensing:
  - https://talonazuremicroservices.azurewebsites.net
  - https://talonlicensing.table.core.windows.net

Networking

- Firewall: TCP ports should be allowed between Global File Cache Edge and Core instances.
- Global File Cache TCP Ports: 443 (HTTPS), 6618–6630.
- Network optimization devices (such as Riverbed Steelhead) must be configured to pass-thru Global File Cache specific ports (TCP 6618-6630).

Getting started

You use Cloud Manager to deploy the Global File Cache Management Server and Global File Cache Core software in the working environment.

Enable Global File Cache using Cloud Manager

In this configuration you will deploy the Global File Cache Management Server and Global File Cache Core in the same working environment where you created your Cloud Volumes ONTAP system using Cloud Manager.

Watch this video to see the steps from start to finish.

Quick start

Get started quickly by following these steps or scroll down to the remaining sections for full details:

1. **Deploy Cloud Volumes ONTAP**

Deploy Cloud Volumes ONTAP in Azure or AWS and configure SMB file shares. For more information, see Launching Cloud Volumes ONTAP in Azure or Launching Cloud Volumes ONTAP in AWS.

2. **Deploy the Global File Cache Management Server**

Deploy an instance of the Global File Cache Management Server in the same working environment as the instance of Cloud Volumes ONTAP.

3. **Deploy the Global File Cache Core**

Deploy an instance, or multiple instances, of the Global File Cache Core in the same working environment as the instance of Cloud Volumes ONTAP and join it to your Active Directory domain.

4. **License Global File Cache**

Configure the Global File Cache License Management Server (LMS) service on a Global File Cache Core instance. You will need your NSS Credentials or a Customer ID and Subscription Number provided by NetApp to activate your subscription.

5. **Deploy the Global File Cache Edge instances**

See Deploying Global File Cache Edge instances to deploy the Global File Cache Edge instances in each remote location. This step is not done using Cloud Manager.

Deploy Cloud Volumes ONTAP as your storage platform

In the current release, Global File Cache supports Cloud Volumes ONTAP deployed in Azure or AWS. For detailed prerequisites, requirements, and deployment instructions, see Launching Cloud Volumes ONTAP in Azure or Launching Cloud Volumes ONTAP in AWS.

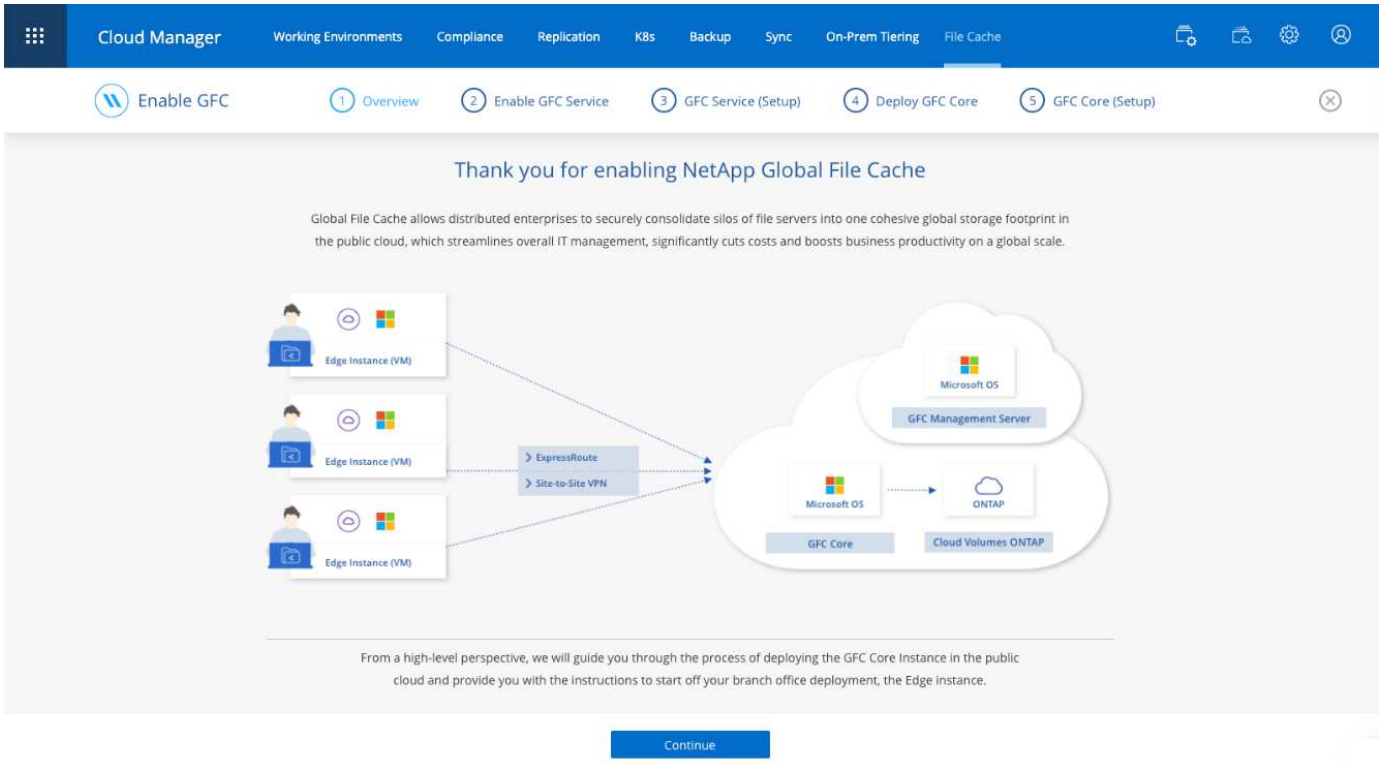
Note the following additional Global File Cache requirement:

- You should configure SMB file shares on the instance of Cloud Volumes ONTAP.

  If no SMB file shares are set up on the instance, then you are prompted to configure the SMB shares during the installation of the Global File Cache components.

Enable Global File Cache in your working environment

The Global File Cache wizard walks you through the steps to deploy the Global File Cache Management Server instance and the Global File Cache Core instance, as highlighted below.



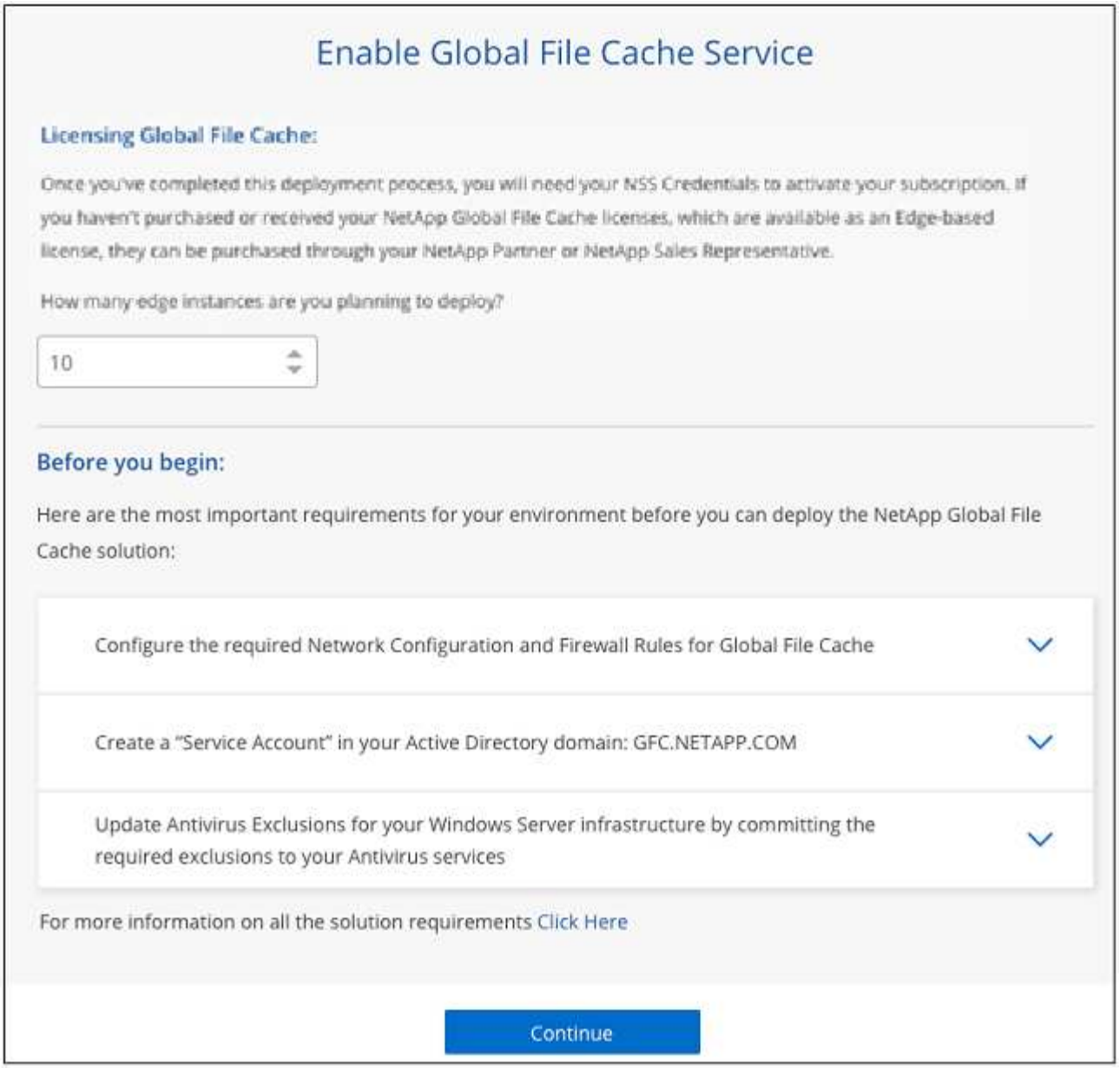
Steps

1. Select the working environment where you deployed Cloud Volumes ONTAP.
2. In the Services panel, click **Enable GFC**.

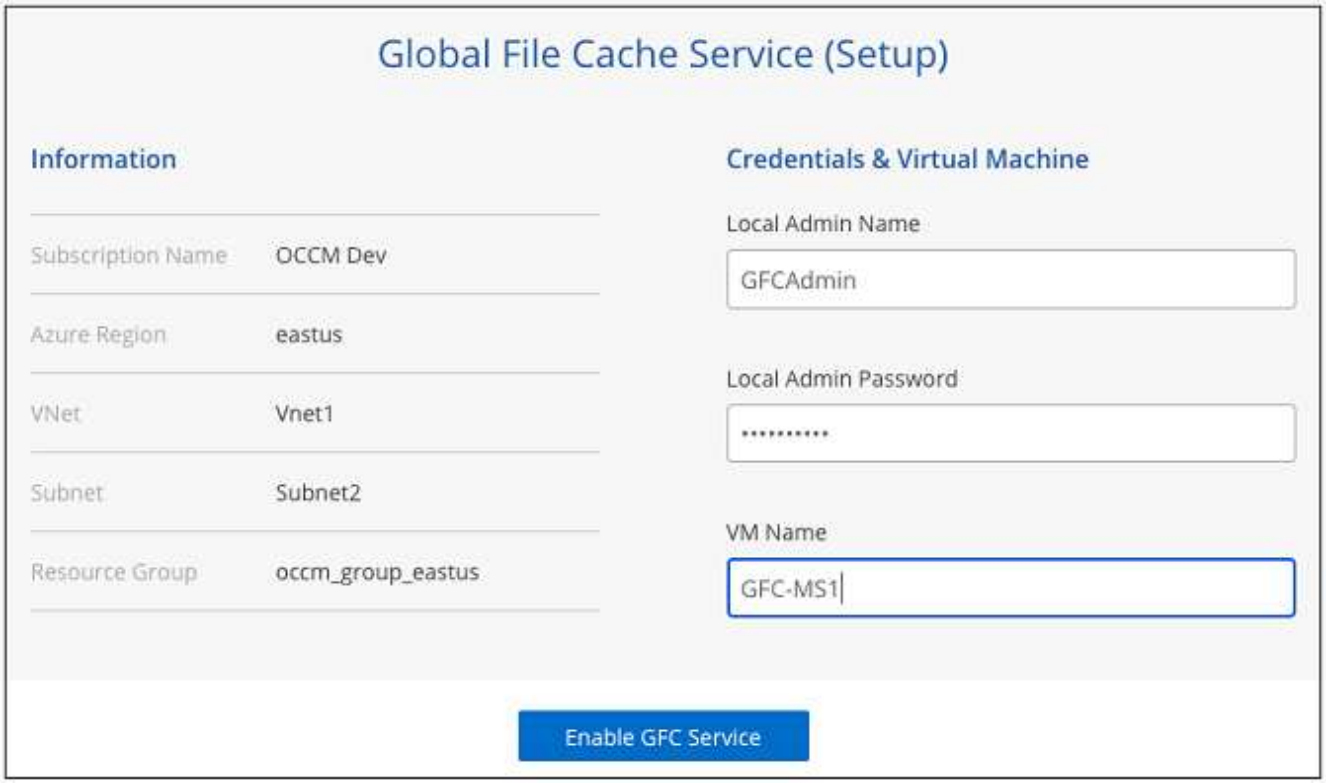
3. Read the Overview page and click **Continue**.
4. If no SMB shares are available on the Cloud Volumes ONTAP instance, you are prompted to enter the SMB Server and SMB Share details to create the share now. For details about the SMB configuration, see Storage platform.

   When finished, click **Continue** to create the SMB share.

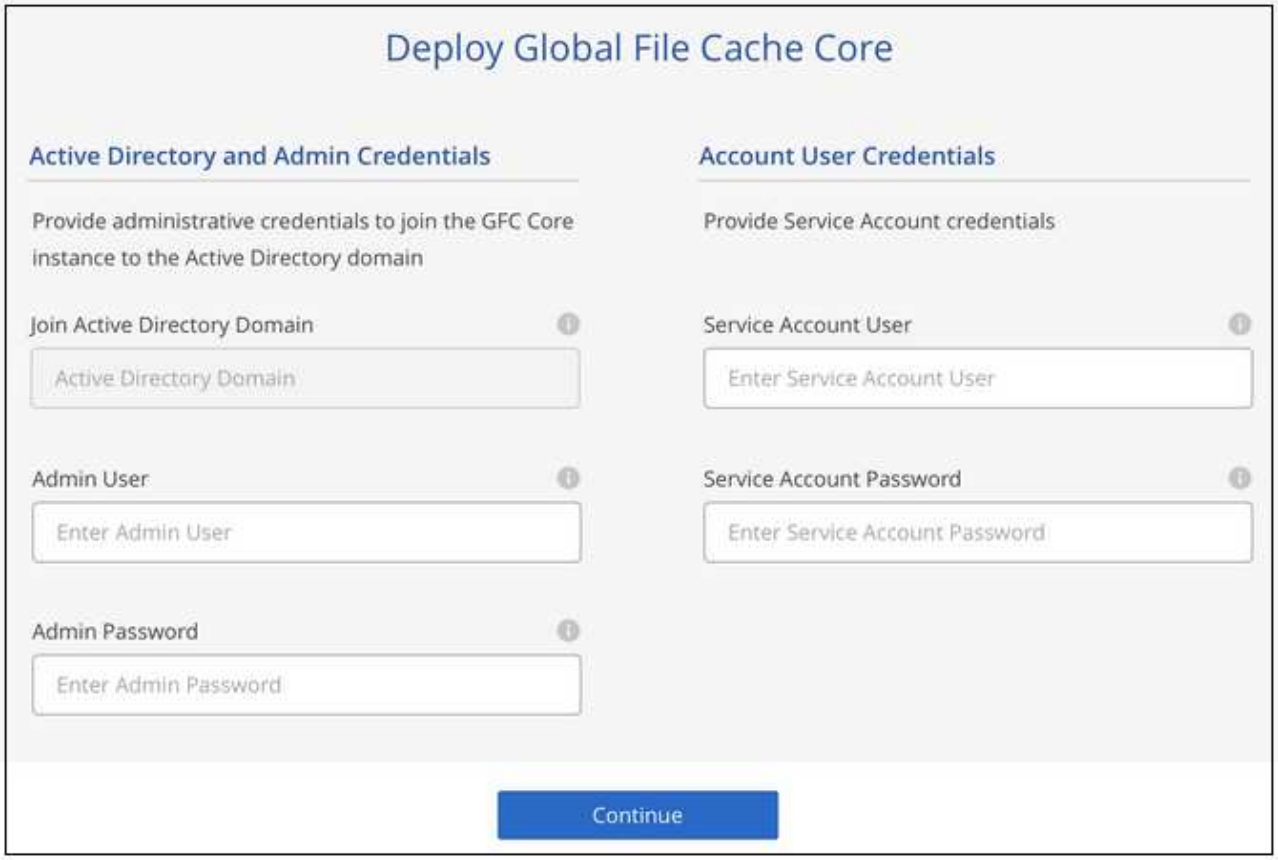
5. On the Global File Cache Service page, enter the number of Global File Cache Edge instances you plan to deploy, and then make sure your system meets the requirements for Network Configuration and Firewall Rules, Active Directory settings, and Antivirus exclusions. See Prerequisites for more details.



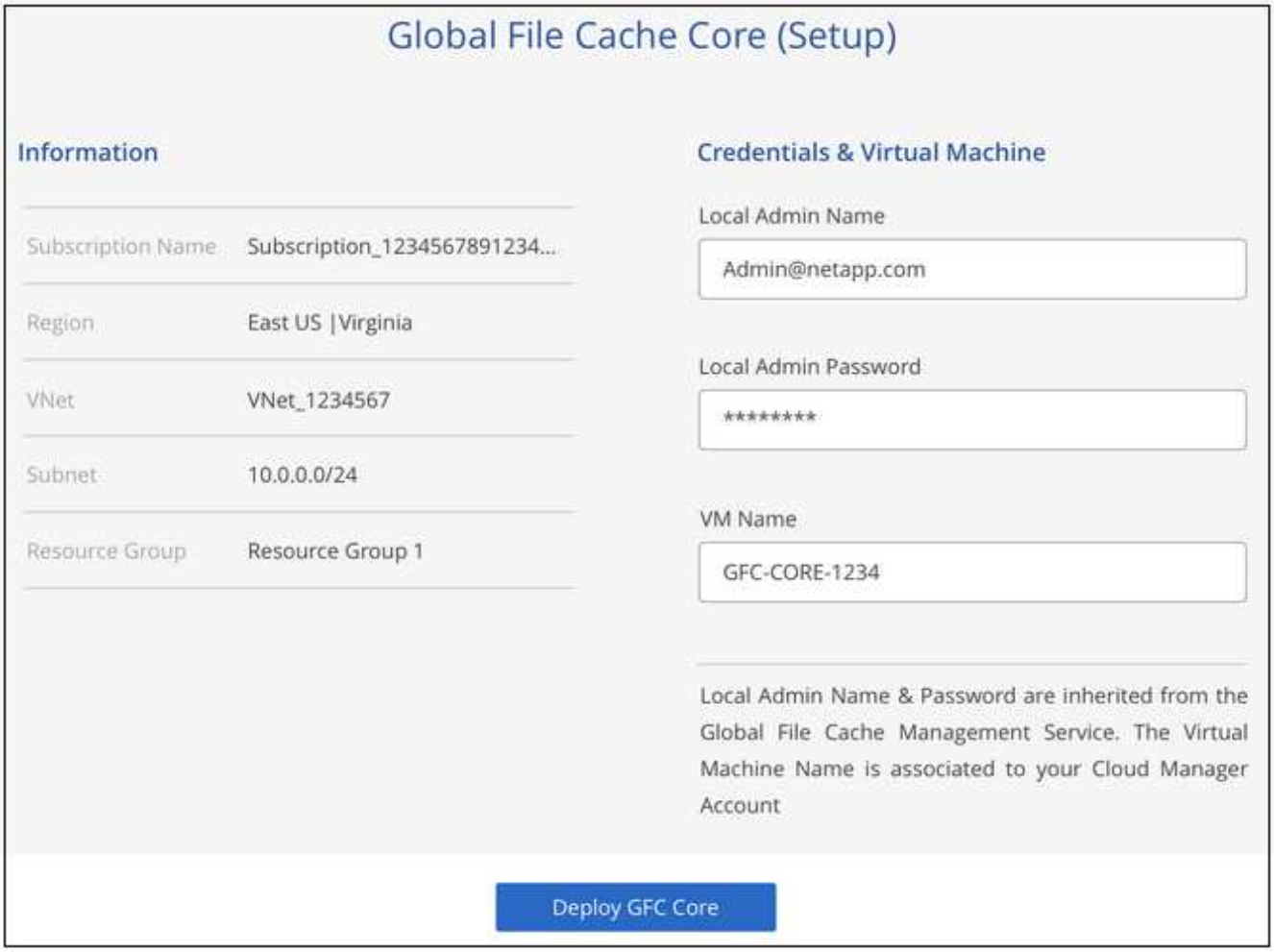
6. After you have verified that the requirements have been met, or that you have the information to meet these requirements, click **Continue**.
7. Enter the admin credentials you will use to access to the Global File Cache Management Server VM and click **Enable GFC Service**. For Azure you enter the credentials as a user name and password; for AWS you select the appropriate key pair. You can change the VM/instance name if you want.



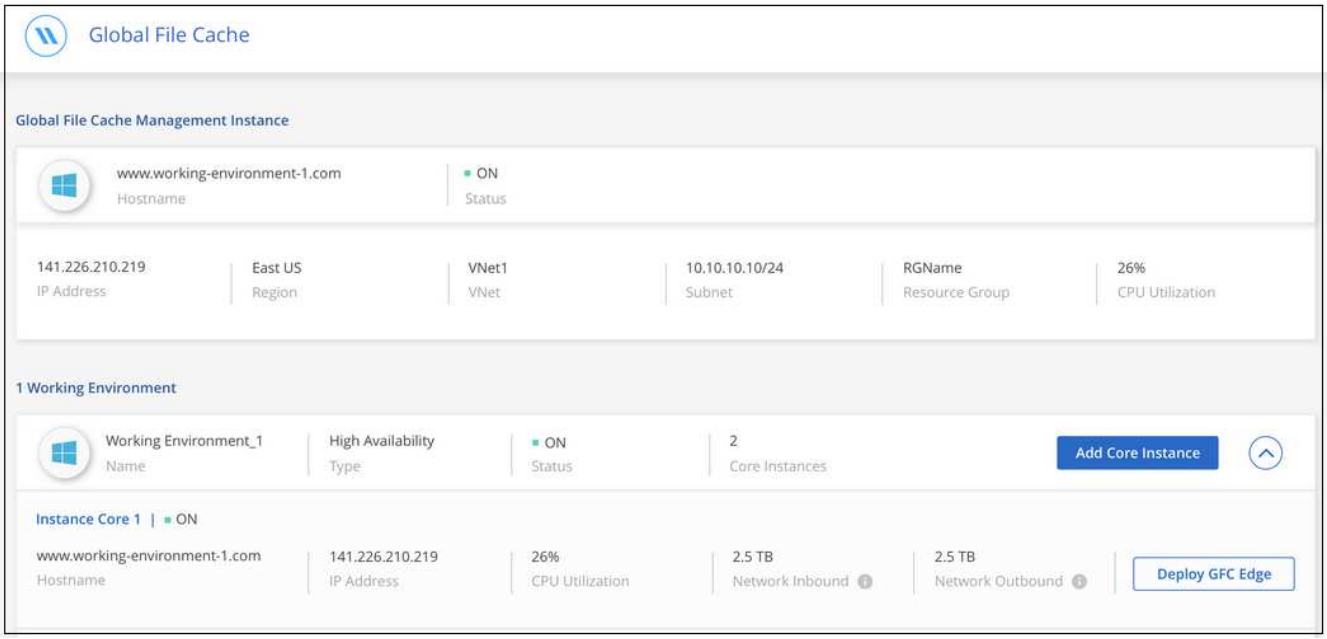
8. After the Global File Cache Management Service is successfully deployed, click **Continue**.
9. For the Global File Cache Core, enter the admin user credentials to join the Active Directory domain, and the service account user credentials. Then click **Continue**.
    - The Global File Cache Core instance must be deployed in the same Active Directory domain as the Cloud Volumes ONTAP instance.
    - The service account is a domain user and it is part of the BUILTIN\Backup Operators group on the Cloud Volumes ONTAP instance.



10. Enter the admin credentials you will use to access to the Global File Cache Core VM and click **Deploy GFC Core**. For Azure you enter the credentials as a user name and password; for AWS you select the appropriate key pair. You can change the VM/instance name if you want.



11. After the Global File Cache Core is successfully deployed, click **Go to Dashboard**.



The Dashboard shows that the Management Server instance and the Core instance are both **On** and working.

License your Global File Cache installation

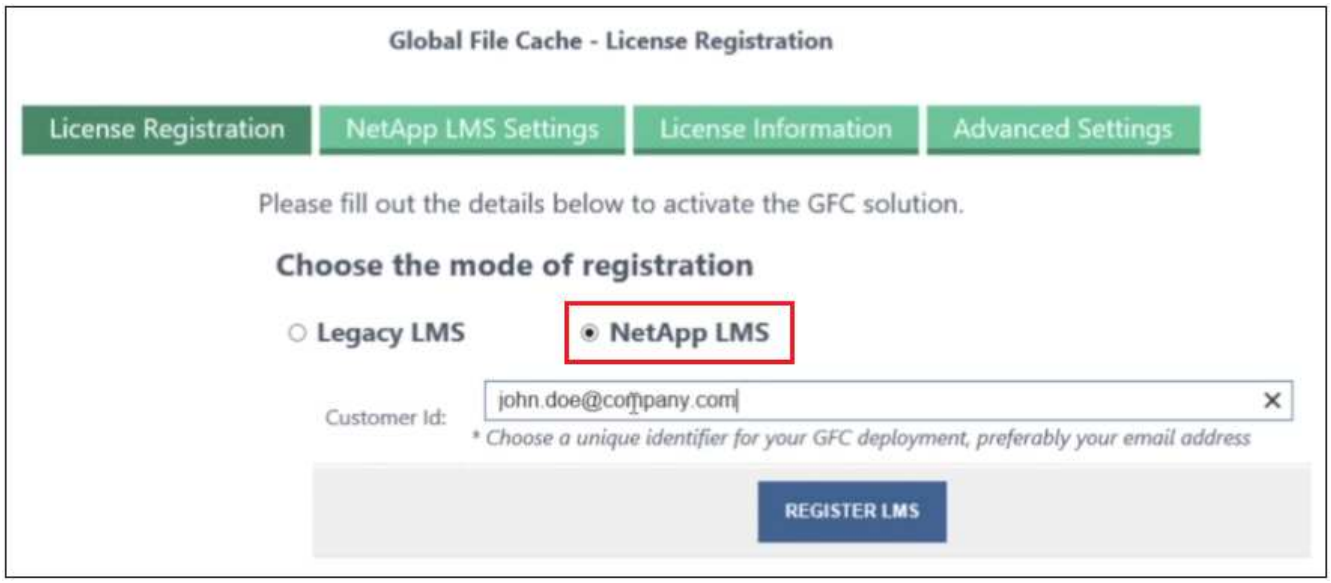
Before you can use Global File Cache, you need to configure the Global File Cache License Management Server (LMS) service on a Global File Cache Core instance. You will need your NSS Credentials or a Customer ID and Subscription Number provided NetApp to activate your subscription.

In this example, we will configure the LMS service on a Core instance that you just deployed in the public cloud. This is a one-time process that sets up your LMS service.

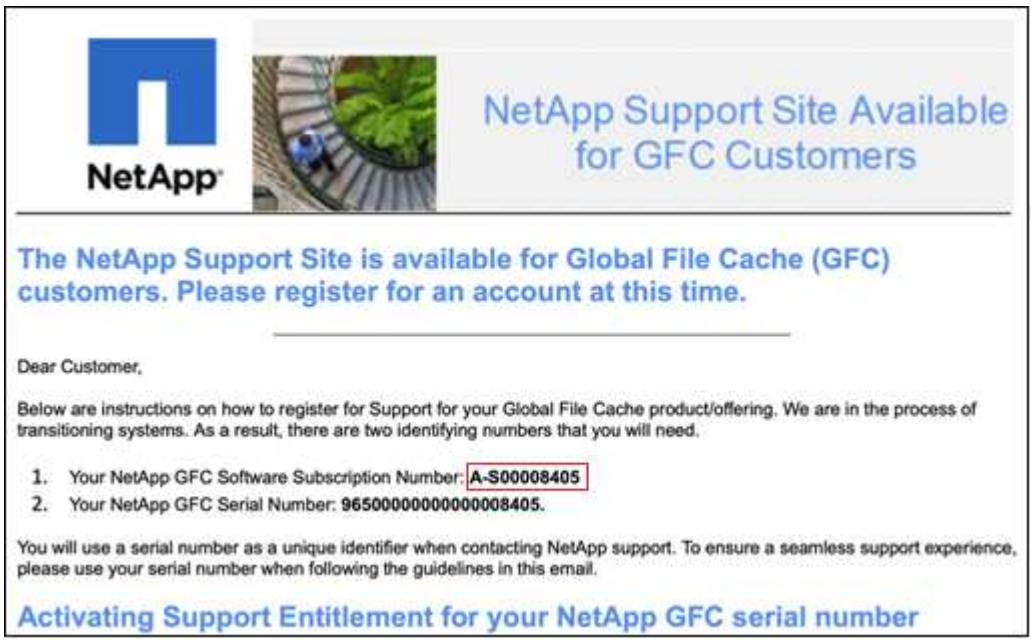
Steps

1. Open the Global File Cache License Registration page on the Global File Cache Core (the Core you are designating as your LMS service) using the following URL. Replace *<ip_address>* with the IP address of the Global File Cache Core:
   https://<ip_address>/lms/api/v1/config/lmsconfig.html
2. Click **"Continue to this website (not recommended)"** to continue. A page that allows you to configure the LMS, or check existing license information, is displayed.

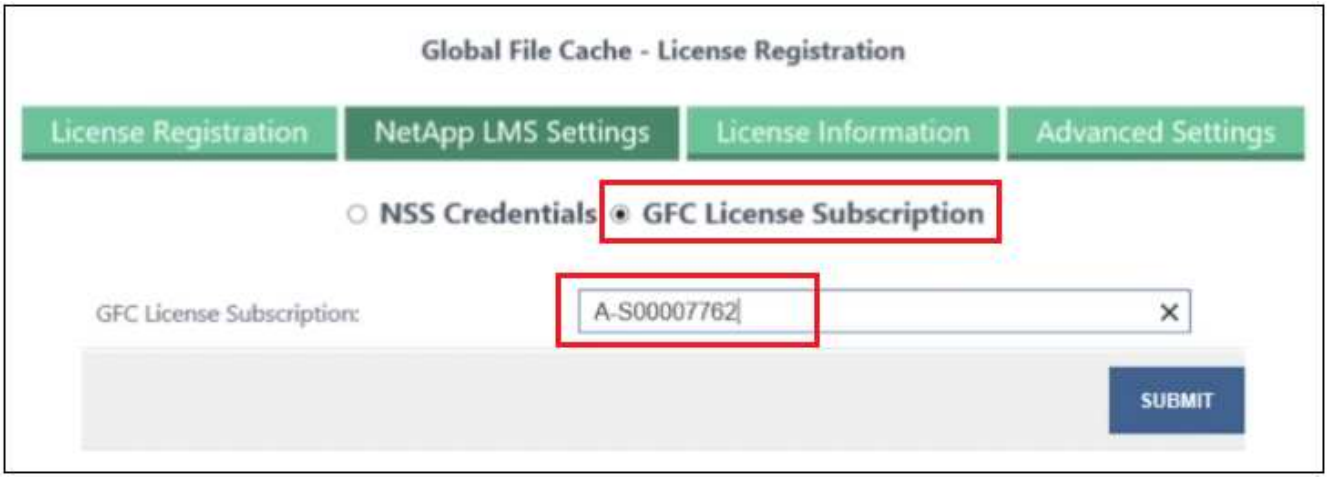
3. Choose the mode of registration:
   - "NetApp LMS" is used for customers who have purchased NetApp Global File Cache Edge licenses from NetApp or its certified partners. (Preferred)
   - "Legacy LMS" is used for existing or trial customers who have received a Customer ID through NetApp Support. (This option has been deprecated.)
4. For this example, click **NetApp LMS**, enter your Customer ID (preferably your email address), and click **Register LMS**.



5. Check for a confirmation email from NetApp that includes your GFC Software Subscription Number and Serial Number.



6. Click the **NetApp LMS Settings** tab.
7. Select **GFC License Subscription**, enter your GFC Software Subscription Number, and click **Submit**.



You will see a message that your GFC License Subscription was registered successfully and activated for the LMS instance. Any subsequent purchases will automatically be added to the GFC License Subscription.

8. Optionally, you can click the **License Information** tab to view all your GFC license information.

What's Next?

If you have determined that you need to deploy multiple Global File Cache Cores to support your configuration, click **Add Core Instance** from the Dashboard and follow the deployment wizard.

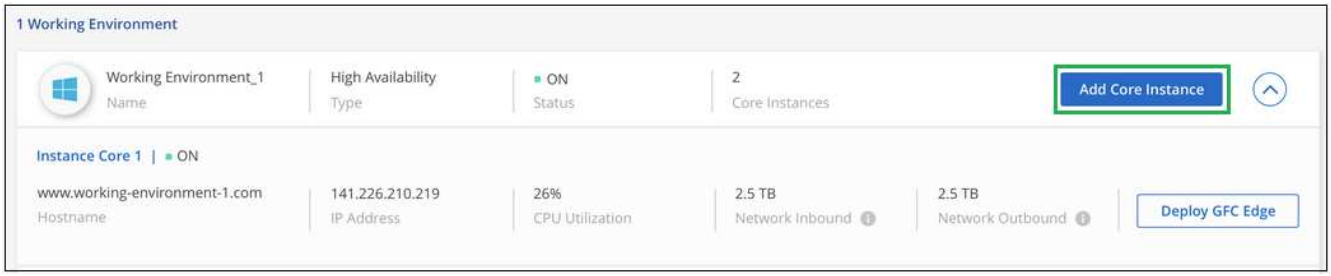
After you have completed your Core deployment, you need to deploy the Global File Cache Edge instances in each of your remote offices.

Deploy additional Core instances

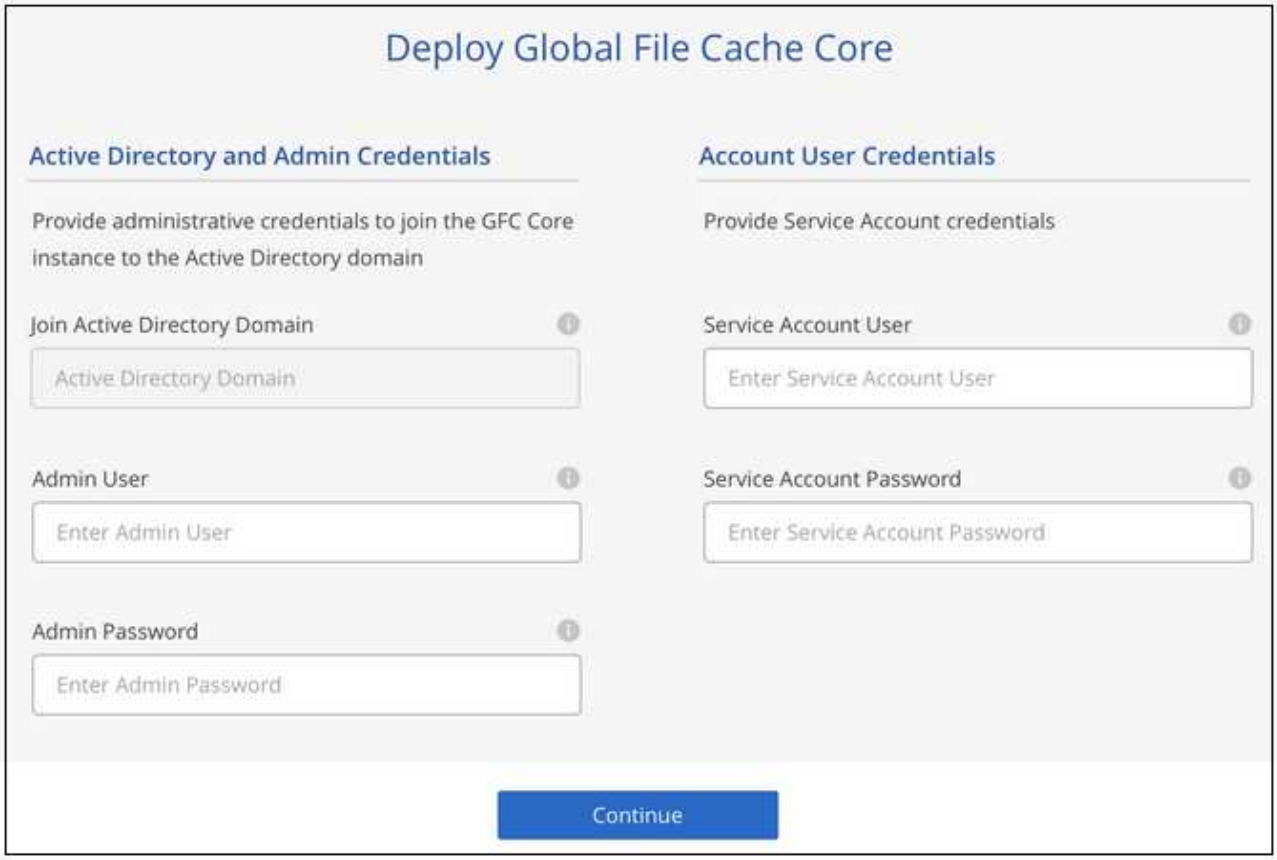
If your configuration requires more than one Global File Cache Core to be installed because of a large number of Edge instances, you can add another Core to the working environment.

When deploying Edge instances, you will configure some to connect to the first Core and others to the second Core. Both Core instances access the same backend storage (your Cloud Volumes ONTAP instance) in the working environment.

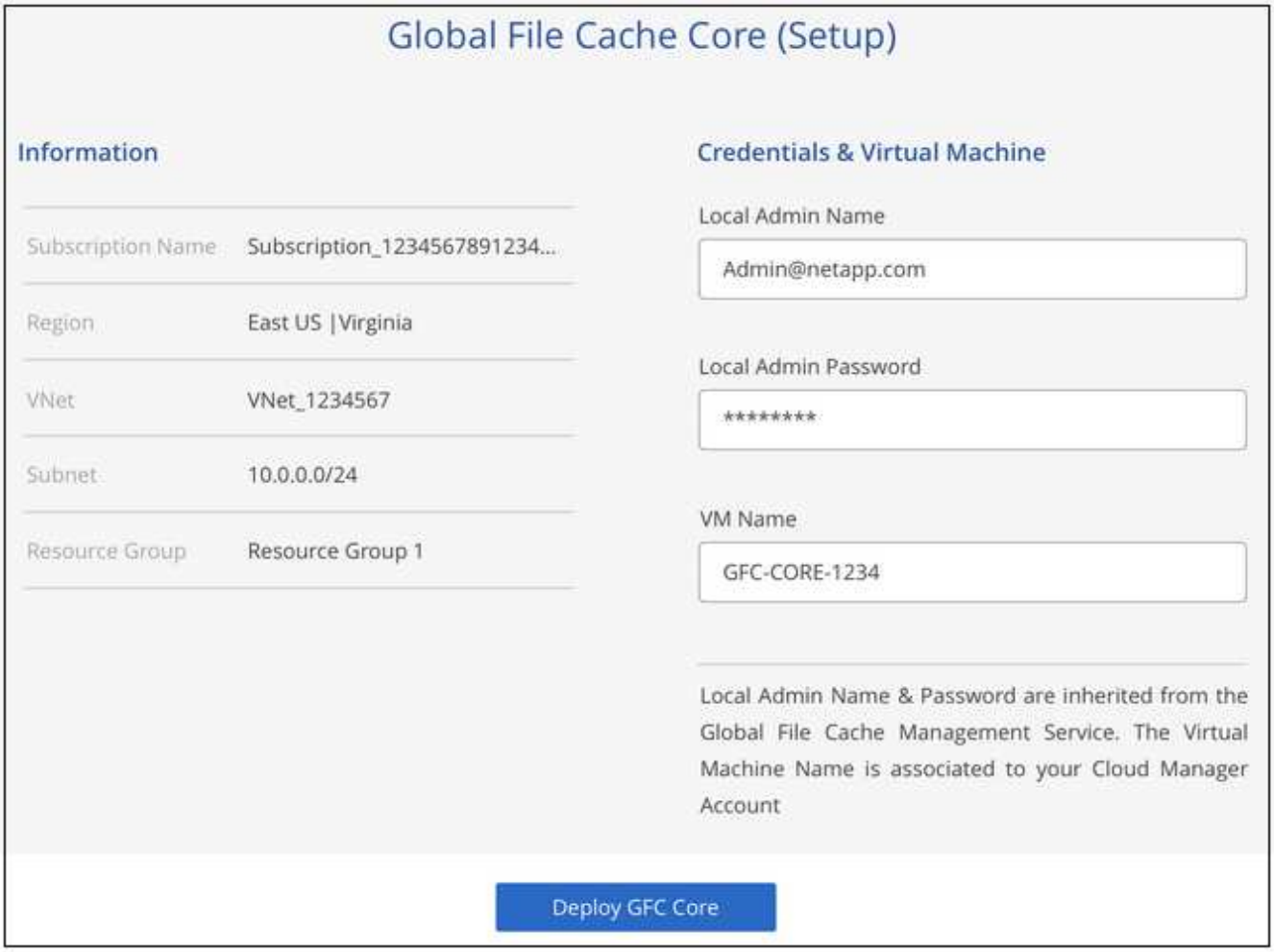
1. From the Global File Cache Dashboard, click **Add Core Instance**.



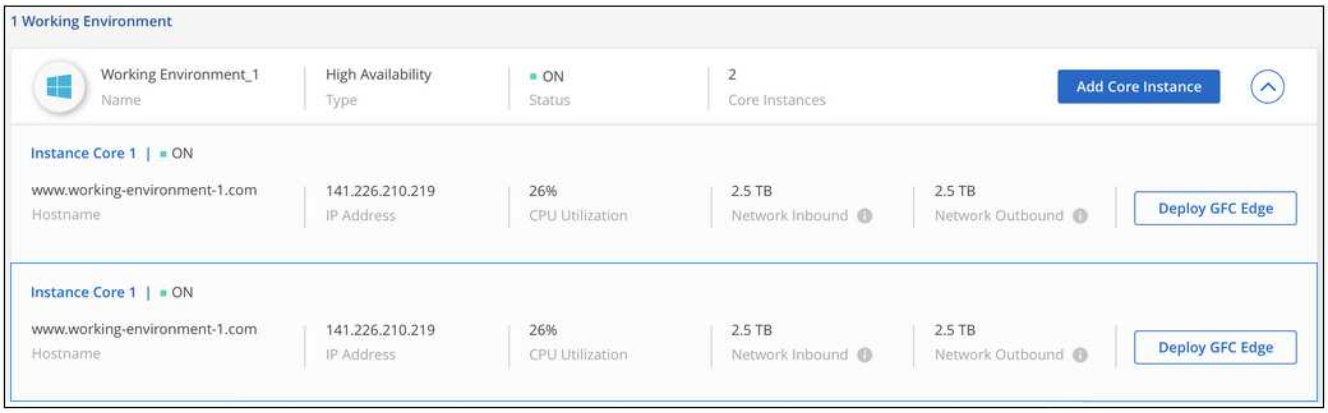
2. Enter the admin user credentials to join the Active Directory domain, and the service account user credentials. Then click **Continue**.
   - The Global File Cache Core instance must be in the same Active Directory domain as the Cloud Volumes ONTAP instance.
   - The service account is a domain user and it is part of the BUILTIN\Backup Operators group on the Cloud Volumes ONTAP instance.



3. Enter the admin credentials you will use to access to the Global File Cache Core VM and click **Deploy GFC Core**. For Azure you enter the credentials as a user name and password; for AWS you select the appropriate key pair. You can change the VM name if you want.



4. After the Global File Cache Core is successfully deployed, click **Go to Dashboard**.



The Dashboard reflects the second Core instance for the working environment.

Before you begin to deploy Global File Cache Edge instances

There are many requirements you need to be aware of before you begin to install Global File Cache Edge software in your remote offices.

Download required resources

Download the Global File Cache Virtual Templates you are planning to use in your branch offices, the software installation package, and additional reference documentation:

- Windows Server 2016 Virtual Template:

  Windows Server 2016 .OVA including NetApp GFC (VMware VSphere 6.5+)
  Windows Server 2016 .VHDX including NetApp GFC (Microsoft Hyper-v)

- Windows Server 2019 Virtual Template:

  Windows Server 2019 .OVA including NetApp GFC (VMware VSphere 6.5+)
  Windows Server 2019 .VHDX including NetApp GFC (Microsoft Hyper-v)

- Global File Cache Edge Software:

  NetApp GFC Software Installation Package (.EXE)

- Global File Cache SCOM (Microsoft Systems Center Operations Manager) Package:

  NetApp GFC SCOM Management Package (.ZIP)

- Global File Cache Documentation:

  NetApp Global File Cache User Guide (.PDF)

Designing and deploying Global File Cache Edge

Depending on your requirements, you might need to deploy one or multiple Global File Cache Edge instances based on the concurrent user sessions in a branch office. The Edge instance presents the virtual file share to the end users within the branch office, which has been transparently extended from the associated Global File Cache Core instance. The Global File Cache Edge should contain a `D:\` NTFS volume, which contains the cached files within the branch office.

> For the Global File Cache Edge, it is important to understand the sizing guidelines. This will assist you in making the correct design for your Global File Cache deployment. You would also need to determine what's right for your environment in terms of scale, availability of resources, and in terms of redundancy.

Global File Cache Edge instance

When deploying a Global File Cache Edge instance, you need to provision a single VM, either by deploying Windows Server 2016 Standard or Datacenter Edition, or Windows Server 2019 Standard or Datacenter Edition, or using the Global File Cache `.OVA` or `.VHD` template, which includes the Windows Server operating system of choice and Global File Cache software.

Quick steps

1. Deploy the Global File Cache Virtual Template, or Windows Server 2016 VM, or Windows Server 2019 Standard or Datacenter edition.
2. Ensure the VM is connected to the network, joined to the domain, and accessible through RDP.

3. Install the latest Global File Cache Edge software.
4. Identify the Global File Cache Management Server and Core instance.
5. Configure the Global File Cache Edge instance.

Global File Cache Edge requirements

Global File Cache Edge is designed to function across all platforms supporting Windows Server 2016 and 2019, bringing simplified IT to corporate remote offices and beyond. Critically, Global File Cache can be deployed on your existing hardware infrastructure, virtualization, or hybrid/public cloud environments in almost every case if they meet a few base-level requirements.

Global File Cache Edge requires the following hardware and software resources to function optimally. For more information about overall sizing guidelines, see Sizing guidelines.

Hardened server appliance

The Global File Cache installation package creates a hardened software appliance on any Microsoft Windows Server instance. *Do Not Uninstall* the Global File Cache Package. Uninstalling Global File Cache will impact the functionality of the server instance and might require a full rebuild of the server instance.

Physical hardware requirements

- Minimum 4 CPU cores
- Minimum 16 GB RAM
- Dedicated single or redundant 1 Gbps NIC
- 10k RPM SAS HDD or SSD (preferred)
- RAID controller with write-back caching functionality enabled

Virtual deployment requirements

Hypervisor platforms are known to be subject to performance degradation from a storage subsystem perspective (for example, latency). For optimal performance using Global File Cache, a physical server instance with SSD is recommended.

For best performance in virtual environments, in addition to the physical host requirements, the following requirements and resource reservations must be met:

Microsoft Hyper-V 2012 R2 and later:

- Processor (CPU): CPUs must be set as **Static**: Minimum: 4 vCPU cores.
- Memory (RAM): Minimum: 16 GB set as **Static**.
- Hard-disk provisioning: Hard Disks must be configured as **Fixed Disk**.

VMware vSphere 6.x and later:

- Processor (CPU): Reservation of CPU Cycles must be set. Minimum: 4 vCPU cores @ 10000 MHz.
- Memory (RAM): Minimum: Reservation of 16 GB.
- Hard-disk provisioning:
  - Disk Provisioning must be set as **Thick Provisioned Eager Zeroed**.

    - Hard Disk Shares must be set to **High**.
    - Devices.hotplug must be set to **False** using the vSphere Client to prevent Microsoft Windows from presenting Global File Cache drives as removable.
- Networking: Network Interface must be set to **VMXNET3** (may require VM Tools).

Global File Cache runs on Windows Server 2016 and 2019, hence the virtualization platform needs to support the operating system, as well as integration with utilities enhancing the performance of the VM's guest operating system and management of the VM, such as VM Tools.

Partition sizing requirements

- C:\ - minimum 250 GB (system/boot volume)
- D:\ - minimum 1 TB (separate data volume for Global File Cache Intelligent File Cache*)

*Minimum size is 2x the active data set. The cache volume (D:\) can be extended and is only restricted by the limitations of the Microsoft Windows NTFS file system.

Global File Cache Intelligent File Cache disk requirements

Disk Latency on the Global File Cache Intelligent File Cache disk (D:\) should deliver < 0.5ms average I/O disk latency and 1MiBps throughput per concurrent user.

For more information, see the NetApp Global File Cache User Guide.

Networking

- Firewall: TCP ports should be allowed between the Global File Cache Edge and Management Server and Core instances.

  Global File Cache TCP Ports: 443 (HTTPS - LMS), 6618 – 6630.

- Network optimization devices (such as Riverbed Steelhead) must be configured to pass-thru Global File Cache specific ports (TCP 6618-6630).

Client workstation and application best practices

Global File Cache transparently integrates into customer's environments, allowing users to access centralized data using their client workstations, running enterprise applications. Using Global File Cache, data is accessed through a direct drive mapping or through a DFS namespace. For more information about the Global File Cache Fabric, Intelligent File Caching, and key aspects of the software, consult the Before you begin to Deploy Global File Cache section.

To ensure an optimal experience and performance, it is important to comply with the Microsoft Windows Client requirements and best practices as outlined in the Global File Cache User Guide. This applies to all versions of Microsoft Windows.

For more information, see the NetApp Global File Cache User Guide.

Firewall and Antivirus best practices

While Global File Cache makes a reasonable effort to validate that the most common antivirus application suites are compatible with Global File Cache, NetApp cannot guarantee and is not responsible for any incompatibilities or performance issues caused by these programs, or their associated updates, service packs,

or modifications.

Global File Cache does not recommend the installation nor application of monitoring or antivirus solutions on any Global File Cache enabled instance (Core or Edge). Should a solution be installed, by choice or by policy, the following best practices and recommendations must be applied. For common antivirus suites, see Appendix A in the NetApp Global File Cache User Guide.

Firewall settings

- Microsoft firewall:
  - Retain firewall settings as default.
  - Recommendation: Leave Microsoft firewall settings and services at the default setting of OFF, and not started for standard Global File Cache Edge instances.
  - Recommendation: Leave Microsoft firewall settings and services at the default setting of ON, and started for Edge instances that also run the Domain Controller role.
- Corporate firewall:
  - Global File Cache Core instance listens on TCP ports 6618-6630, ensure that Global File Cache Edge instances can connect to these TCP ports.
  - Global File Cache instances require communications to the Global File Cache Management Server on TCP port 443 (HTTPS).
- Network optimization solutions/devices must be configured to pass-thru Global File Cache specific ports.

Antivirus best practices

This section helps you to understand the requirements when running antivirus software on a Windows Server instance running Global File Cache. Global File Cache has tested most commonly used antivirus products including Cylance, McAfee, Symantec, Sophos, Trend Micro, Kaspersky and Windows Defender for use in conjunction with Global File Cache.

> Adding antivirus to an Edge appliance can introduce a 10–20% impact on user performance.

For more information, see the NetApp Global File Cache User Guide.

Configure exclusions

Antivirus software or other third-party indexing or scanning utilities should never scan drive D:\ on the Edge instance. These scans of Edge server drive D:\ will result in numerous file open requests for the entire cache namespace. This will result in file fetches over the WAN to all file servers being optimized at the data center. WAN connection flooding and unnecessary load on the Edge instance will occur resulting in performance degradation.

In addition to the D:\ drive, the following Global File Cache directory and processes should generally be excluded from all antivirus applications:

- `C:\Program Files\TalonFAST\`
- `C:\Program Files\TalonFAST\Bin\LMClientService.exe`
- `C:\Program Files\TalonFAST\Bin\LMServerService.exe`
- `C:\Program Files\TalonFAST\Bin\Optimus.exe`

- `C:\Program Files\TalonFAST\Bin\tafsexport.exe`
- `C:\Program Files\TalonFAST\Bin\tafsutils.exe`
- `C:\Program Files\TalonFAST\Bin\tapp.exe`
- `C:\Program Files\TalonFAST\Bin\TappN.exe`
- `C:\Program Files\TalonFAST\Bin\FTLSummaryGenerator.exe`
- `C:\Program Files\TalonFAST\Bin\RFASTSetupWizard.exe`
- `C:\Program Files\TalonFAST\Bin\TService.exe`
- `C:\Program Files\TalonFAST\Bin\tum.exe`
- `C:\Program Files\TalonFAST\FastDebugLogs\`
- `C:\Windows\System32\drivers\tfast.sys`
- `\\?\TafsMtPt:\` or `\\?\TafsMtPt*`
- `\Device\TalonCacheFS\`
- `\\?\GLOBALROOT\Device\TalonCacheFS\`
- `\\?\GLOBALROOT\Device\TalonCacheFS\*`

NetApp Support policy

Global File Cache instances are designed specifically for Global File Cache as the primary application running on a Windows Server 2016 and 2019 platform. Global File Cache requires priority access to platform resources, for example, disk, memory, network interfaces, and can place high demands on these resources. Virtual deployments require memory/CPU reservations and high-performance disks.

- For branch office deployments of Global File Cache, supported services and applications on the server running Global File Cache are limited to:
  - DNS/DHCP
  - Active Directory domain controller (Global File Cache must be on a separate volume)
  - Print services
  - Microsoft System Center Configuration Manager (SCCM)
  - Global File Cache approved client-side system agents and anti-virus applications
- NetApp Support and maintenance applies only to Global File Cache.
- Line of business productivity software, which are typically resource intensive, for example, database servers, mail servers, and so on, are not supported.
- The customer is responsible for any non-Global File Cache software which might be installed on the server running Global File Cache:
  - If any third-party software package causes software or resource conflicts with Global File Cache or performance is compromised, Global File Cache's support organization might require the customer to disable or remove the software from the server running Global File Cache.
  - It is the customer's responsibility for all installation, integration, support, and upgrade of any software added to the server running the Global File Cache application.
- Systems management utilities/agents such as antivirus tools and licensing agents might be able to coexist. However, except for the supported services and applications listed above, these applications are not

supported by Global File Cache and the same guidelines as above must still be followed:

- It is the customer's responsibility for all installation, integration, support, and upgrade of any software added.
- If a customer does install any third-party software package that causes, or is suspected to be causing, software or resource conflicts with Global File Cache or performance is compromised, there might be a requirement by Global File Cache's support organization to disable/remove the software.

Deploy Global File Cache Edge instances

After you have verified that your environment meets all the requirements, you install Global File Cache Edge software in each remote office.

Before you begin

To complete Global File Cache Edge configuration tasks, you need the following information:

- Static IP addresses for each Global File Cache instance
- Subnet mask
- Gateway IP address
- The FQDN you wish to assign to each Global File Cache server
- The DNS suffix (optional)
- The user name and password of an administrative user in the domain
- The FQDN and/or IP address of the associated Core servers
- A volume to be used as the Intelligent File Cache. It is recommended this be at least 2x the size of the active dataset. This should be formatted as NTFS and assigned as `D:\`.

Commonly used TCP ports

There are several TCP ports used by Global File Cache services. It is mandatory that the devices can communicate on these ports and they be excluded from any WAN optimization devices or firewall restriction policies:

- Global File Cache Licensing TCP Port: 443
- Global File Cache TCP Ports: 6618-6630

Deploy the Global File Cache Virtual Template

The virtual template (`.OVA` and `.VHD`) images contain the latest release of the Global File Cache software. If you are deploying Global File Cache using the `.OVA` or `.VHD` virtual machine (VM) template, follow the steps as outlined in this section. It is assumed that you understand how to deploy the `.OVA` or `.VHD` template on the designated hypervisor platform.

Ensure that VM preferences, including resource reservations, are in line with the requirements as outlined in Virtual deployment requirements.

Steps

1. Extract the package from the template you downloaded.

2. Deploy the virtual template. Refer to the following videos before you start the deployment:
    - Deploy the Virtual Template on VMware
    - Deploy the Virtual Template on Hyper-V
3. After the Virtual Template has been deployed, and you have configured the VM settings, start the VM.
4. During initial boot, when the Windows Server 2016 or 2019 operating system is preparing for first use, complete the out-of-the-box experience by installing the correct drivers and installing the necessary components for the respective hardware.
5. When the base install of the Global File Cache Edge instance has been completed, the Windows Server 2016 or 2019 operating system will guide you through an initial configuration wizard to configure operating system specifics such as localization and product key.
6. After the initial configuration wizard has completed, log in locally to the Windows Server 2016 or 2019 operating system with the following credentials:
    - User name: **FASTAdmin**
    - Password: **Tal0nFAST!**
7. Configure your Windows Server VM, join to the organization's Active Directory domain, and proceed to the Global File Cache Edge configuration section.

Configure the Global File Cache Edge instance

The Global File Cache Edge instance connects to a Global File Cache Core to provide users at the branch office access to data center file server resources.

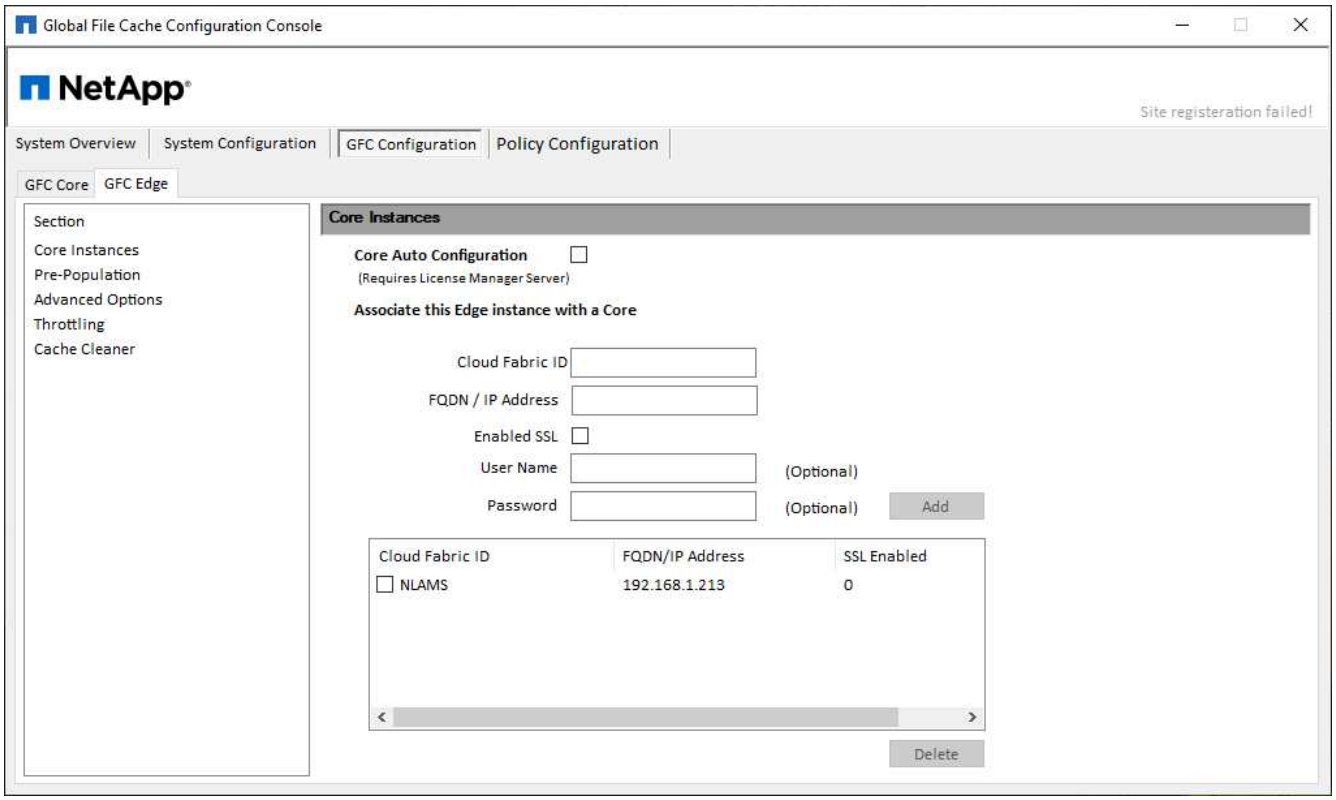
> The Edge instance must be licensed as part of your Cloud Volumes ONTAP deployment prior to beginning the configuration. See Licensing for more information about licensing.

If your configuration requires more than one Global File Cache Core to be installed because of a large number of Edge instances, you will configure some Edge instances to connect to the first Core and others to connect to the second Core. Make sure you have the FQDN or IP address, and other required information, for the correct Core instance.

To configure the Edge instance, complete the following steps:

Steps

1. Click **Perform** next to the unchecked Core Configuration step listed in the "Edge Configuration Steps" section of the Initial Configuration assistant. This opens a new tab, GFC Edge, and shows the section *Core Instances*.
2. Provide the **Cloud Fabric ID** of the Global File Cache Core server. The Cloud Fabric ID is typically the NetBIOS name or the geographical location of the backend file server.
3. Provide the **FQDN/IP Address** of the Global File Cache Core server:
    a. (Optional) Check the **SSL** box to enable SSL support for enhanced encryption from the Edge to the Core.
    b. Enter the User Name and Password, which are the credentials of the Service Account used on the Core.
4. Click **Add** to confirm the addition of the Global File Cache Core appliance. A confirmation box will appear. Click **OK** to dismiss it.



Update Global File Cache Edge software

Global File Cache frequently releases updates to the software, either patches, enhancements, or new features/functionality. Although the virtual template (`.OVA` and `.VHD`) images contain the latest release of the Global File Cache software, it is possible that a newer version is available on the NetApp Support Download portal.

Ensure that your Global File Cache instances are up to date with the latest version.

> This software package can also be used for pristine installations on Microsoft Windows Server 2016 Standard or Datacenter edition, or Windows Server 2019 Standard or Datacenter edition, or used as part of your upgrade strategy.

Below you can find the steps required to update the Global File Cache installation package:

Steps

1. After saving the latest installation package to the desired Windows Server instance, double-click it to run the installation executable.
2. Click **Next** to continue the process.
3. Click **Next** to continue.
4. Accept the Licensing Agreement and click **Next**.
5. Select the desired Installation Destination Location.

   NetApp recommends that you use the default installation location.

6. Click **Next** to continue.
7. Select the Start Menu Folder.

8. Click **Next** to continue.
9. Verify your installation selections and click **Install** to begin the installation.

   The installation process will start.

10. After the installation has completed, reboot the server when prompted.

What's Next?

For details about Global File Cache Edge advanced configuration, see the NetApp Global File Cache User Guide.

Use Global File Cache

End-user training

You will want to train your users on the best practices for accessing the shared files through Global File Cache.

This is the final phase of the Global File Cache deployment, the end-user implementation phase.

In order to prepare and streamline the end user on-boarding process, use the email template below that will help you to educate end users on what it means to work in a "central data" environment. This will help your users leverage all of the benefits of the Global File Cache solution. We have also published a video that can be shared to "train" users where needed.

Customize and forward the following resources to end users to prepare them for roll-out:

- User Training video
  End user training video
- Email Template
  Mac Email Template (.emltpl)

  Windows Email Template (.msg)
- Onboarding Communications
  Word Document (.docx)

See Chapter 13 in the NetApp Global File Cache User Guide for additional material.

Additional information

Use the following links to learn more about Global File Cache and other NetApp products:

- Global File Cache FAQ
  - See a list of frequently asked questions and answers here
- NetApp Global File Cache User Guide
- NetApp Product Documentation
  - See additional documentation for NetApp cloud products here
  - See additional documentation for all NetApp products here
- Customer support for Global File Cache users with Cloud Volumes ONTAP is available through these channels:
  - Guided Problem Solving, Case Management, Knowledgebase, Downloads, Tools, and more go here
  - Login to the NetApp Support at https://mysupport.netapp.com with your NSS credentials
  - For immediate assistance for a P1 issue call: +1 856.481.3990 (Option 2)
- Customer support for Global File Cache users utilizing Cloud Volumes Services and Azure NetApp Files is available through standard support from your provider. Please contact Google Customer Support or Microsoft Customer Support respectively.

Knowledge and support

Register for support

Before you can open a support case with NetApp technical support, you need to add a NetApp Support Site account to Cloud Manager and then register for support.

Add an NSS account

The Support Dashboard enables you to add and manage all of your NetApp Support Site accounts from a single location.

Steps

1. If you don't have a NetApp Support Site account yet, register for one.
2. In the upper right of the Cloud Manager console, click the Help icon, and select **Support**.

   [A screenshot of the Help menu where Support is the first option listed]

3. Click **NSS Management > Add NSS Account**.
4. When you're prompted, click **Continue** to be redirected to a Microsoft login page.

   NetApp uses Microsoft Azure Active Directory as the identity provider for authentication services specific to support and licensing.

5. At the login page, provide your NetApp Support Site registered email address and password to perform the authentication process.

   This action enables Cloud Manager to use your NSS account.

   Note the following requirements for the account:

   - The account must be a customer-level account (not a guest or temp account).
   - If you plan to deploy a node-based BYOL system:
     - The account must be authorized to access the serial numbers of the BYOL systems.
     - If you purchased a secure BYOL subscription, then a secure NSS account is required.

Register your account for support

Support registration is available from Cloud Manager in the Support Dashboard.

Steps

1. In the upper right of the Cloud Manager console, click the Help icon, and select **Support**.

   [A screenshot of the Help menu where Support is the first option listed]

2. In the **Resources** tab, click **Register for Support**.
3. Select the NSS credentials that you want to register and then click **Register**.

Get help

NetApp provides support for Cloud Manager and its cloud services in a variety of ways. Extensive free self-support options are available 24x7, such as knowledgebase (KB) articles and a community forum. Your support registration includes remote technical support via web ticketing.

Self support

These options are available for free, 24 hours a day, 7 days a week:

- Knowledge base

  Search through the Cloud Manager knowledge base to find helpful articles to troubleshoot issues.

- Communities

  Join the Cloud Manager community to follow ongoing discussions or create new ones.

- Documentation

  The Cloud Manager documentation that you're currently viewing.

- Feedback email

  We value your input. Submit feedback to help us improve Cloud Manager.

NetApp support

In addition to the self-support options above, you can work with a NetApp Support Engineer to resolve any issues after you activate support.

Steps

1. In Cloud Manager, click **Help > Support**.
2. Choose one of the available options under Technical Support:
   a. Click **Call Us** to find phone numbers for NetApp technical support.
   b. Click **Open an Issue**, select one the options, and then click **Send**.

      A NetApp representative will review your case and get back to you soon.

Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

Copyright

http://www.netapp.com/us/legal/copyright.aspx

Trademarks

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

http://www.netapp.com/us/legal/netapptmlist.aspx

Patents

A current list of NetApp owned patents can be found at:

https://www.netapp.com/us/media/patents-page.pdf

Privacy policy

https://www.netapp.com/us/legal/privacypolicy/index.aspx

Open source

Notice files provide information about third-party copyright and licenses used in NetApp software.

- Notice for Cloud Manager 3.9
- Notice for Global File Cache

Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.