Before you begin to deploy Global File Cache

Cloud Manager

Tom Onacki, Ben Cammett
July 19, 2021

Table of Contents

Before you begin to deploy Global File Cache 1
Global File Cache Core design considerations 1
Sizing guidelines 1
Prerequisites 2

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).