



Get started

BlueXP edge caching

NetApp
February 11, 2024

Table of Contents

- Get started 1
 - Learn about BlueXP edge caching 1
 - Before you begin to deploy BlueXP edge caching 5
 - Getting started 8
 - Before you begin to deploy BlueXP edge caching Edge instances 20
 - Deploy BlueXP edge caching Edge instances 26

Get started

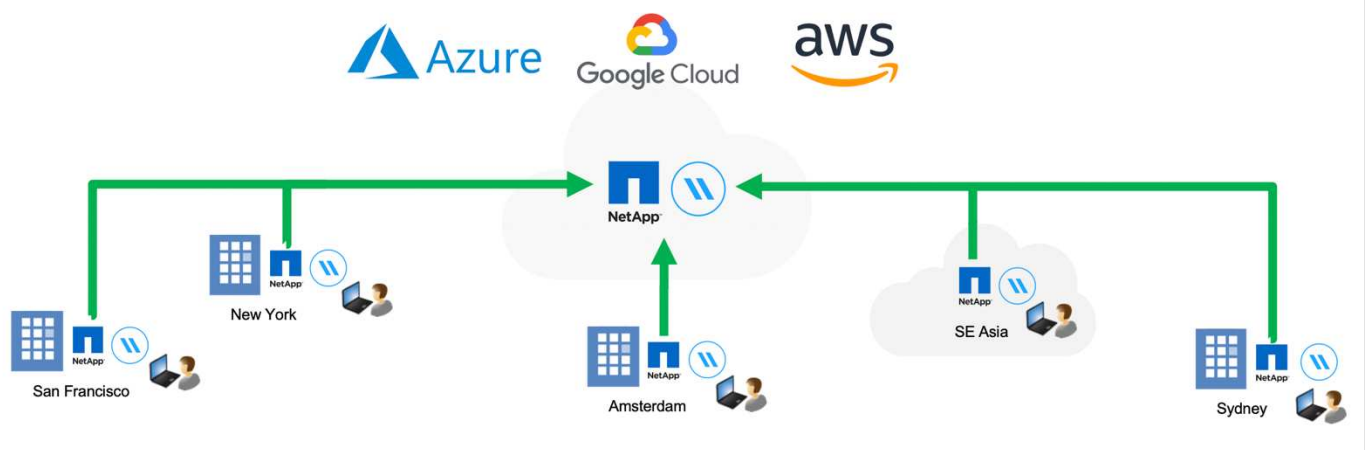
Learn about BlueXP edge caching

NetApp BlueXP edge caching 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.

BlueXP edge caching is available in two deployment modes to fit your enterprise architecture: as an integrated service combined in a Cloud Volumes ONTAP instance (Cloud Volumes Edge Cache), or as an add-on component to your enterprise storage strategy (Global File Cache)

Overview

Implementing BlueXP edge caching 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

BlueXP edge caching 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

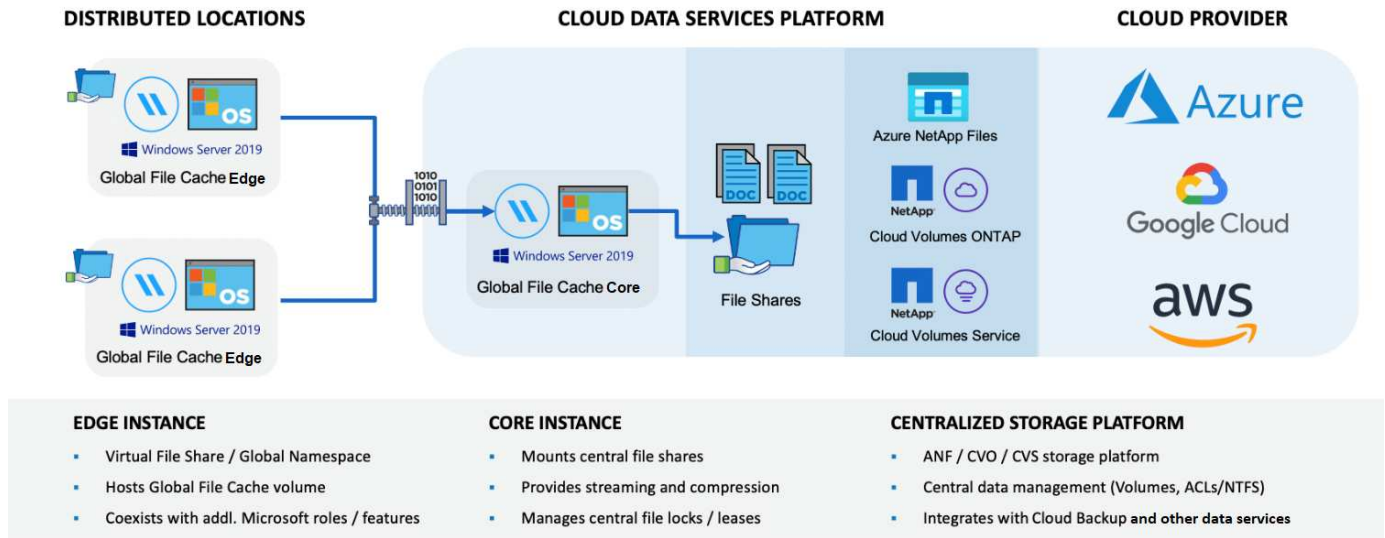
See more about BlueXP edge caching features and use cases [here](#).

BlueXP edge caching components

BlueXP edge caching consists of the following components:

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

The BlueXP edge caching 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 BlueXP edge caching "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 BlueXP edge caching differ depending on the deployment option you select.

Automated deployment options

BlueXP edge caching is supported with the following types of working environments when deployed using BlueXP:

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

This configuration lets you deploy and manage the entire BlueXP edge caching server-side deployment, including BlueXP edge caching Management Server and BlueXP edge caching Core, from within BlueXP.

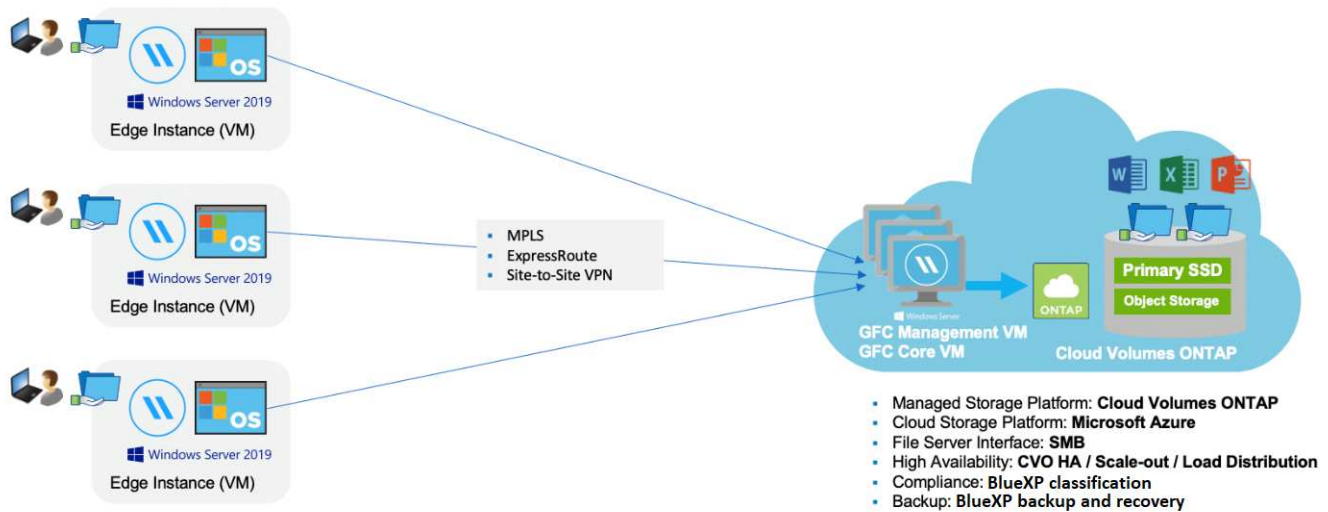
Manual deployment options

BlueXP edge caching configurations are also supported with Cloud Volumes ONTAP, Azure NetApp Files, Amazon FSx for ONTAP systems, and Cloud Volumes Service on Google Cloud. On-premises solutions are also available on NetApp AFF and FAS platforms. In these installations, the BlueXP edge caching server-side components must be configured and deployed manually, not by using BlueXP.

See the [NetApp Global File Cache User Guide](#) for details.

How BlueXP edge caching works

BlueXP edge caching 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
- BlueXP edge caching Fabric:
 - Extension of the central data store to the remote locations
 - BlueXP edge caching Core instance, mounting to corporate file shares (SMB).
 - BlueXP edge caching 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 BlueXP edge caching depends on the type of installation you have chosen.

- All installations require that you deploy one or more volumes in the cloud (for example, 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.
 - BlueXP edge caching Management Server:

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

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

In Google Cloud, this runs on a n2-standard-2 or equivalent (2 vCPU/8 GB RAM) instance with 127 GB general purpose SSD

- BlueXP edge caching Core:

In Azure, this runs on a D8s_V4 or equivalent (8 vCPU/32 GB RAM) VM with 127 GB premium SSD

In AWS, this runs on a m4.2xlarge or equivalent (8 vCPU/32 GB RAM) instance with 127 GB general purpose SSD

In Google Cloud, this runs on a n2-standard-8 or equivalent (8 vCPU/32 GB RAM) instance with 127 GB general purpose SSD

- When installed with Cloud Volumes ONTAP (the supported configurations deployed completely through BlueXP), there are two pricing options:
 - For Cloud Volumes ONTAP systems, you can pay \$3,000 for each BlueXP edge caching Edge instance, per year.
 - Alternatively, for Cloud Volumes ONTAP systems in Azure and GCP, you can choose the Cloud Volumes ONTAP Edge Cache package. This capacity-based license allows you to deploy a single BlueXP edge caching Edge instance for each 3 TiB of purchased capacity. [Learn more here](#).
- 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 NetApp Solutions Engineer to discuss the best options for your enterprise deployment.

Licensing

BlueXP edge caching 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 BlueXP edge caching supported within BlueXP (Cloud Volumes Edge Cache) 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, AWS, or Google Cloud.

Other storage platforms are not supported at this time using BlueXP, but can be deployed using legacy deployment procedures. These other configurations, for example, Global File Cache using Amazon FSx for ONTAP systems, Azure NetApp Files, or Cloud Volumes Service on Google Cloud, are supported using the legacy procedures. See [Global File Cache overview and onboarding](#) for details.

Before you begin to deploy BlueXP edge caching

There are many requirements you need to be aware of before you begin to deploy BlueXP edge caching in the cloud and in your remote offices.

BlueXP edge caching Core design considerations

Depending on your requirements, you may need to deploy one or multiple BlueXP edge caching Core instances to create the BlueXP edge caching Fabric. The Core instance is designed to direct the flow of traffic between your distributed BlueXP edge caching Edge instances and the data center file server resources, for example, file shares, folders, and files.

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

- Stand-alone instance
- 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 NetApp 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:

- Edges/Core ratio
- Distributed users/Edge ratio
- Distributed users/Core ratio

Number of Edge Instances per Core Instance

Our guidelines recommend up to 10 Edge instances per BlueXP edge caching Core instance, with a maximum of 20 Edges per BlueXP edge caching 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 your account representative to determine how to correctly size the number of Edge and Core instances depending on the types and sizes of the file sets.



You can leverage multiple BlueXP edge caching Edge and Core instances simultaneously to scale out your infrastructure depending on the requirements.

Number of concurrent users per Edge instance

The BlueXP edge caching Edge handles the heavy lifting in terms of caching algorithms and file-level differencing. A single Edge instance can serve up to 500 users per dedicated *physical* Edge instance, and up to 300 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 BlueXP edge caching 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 Edge upper boundary (depending on physical or virtual deployment).



The BlueXP edge caching 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 300 or 500 concurrent connections.

Number of concurrent users per Core instance

The BlueXP edge caching 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 NetApp 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 BlueXP edge caching Management Server and the BlueXP edge caching Core.

The BlueXP edge caching Edge prerequisites are described [here](#).

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 BlueXP edge caching 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.

BlueXP edge caching Management Server

The BlueXP edge caching Management Server requires external access over HTTPS (TCP port 443) to connect to the cloud provider subscription service and to access these URLs:

- <https://gfcproxyforcm-prod.azurewebsites.net/>

- <https://rest.zuora.com/v1/subscriptions/>
- <https://rest.zuora.com/oauth/token>
- <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 BlueXP edge caching software to operate properly.

The BlueXP edge caching Management Server also requires a unique (geographical) NetBIOS name for the instance (such as GFC-MS1).



One Management Server can support multiple BlueXP edge caching Core instances deployed in different working environments. When deployed from BlueXP, each working environment has its own separate backend storage and would not contain the same data.

BlueXP edge caching Core

The BlueXP edge caching 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 BlueXP edge caching software to operate properly.

The BlueXP edge caching Core requirements are:

- A unique (geographical) NetBIOS name for the instance (such as GFC-CORE1)
- Active Directory domain name
 - Instances should be joined to your Active Directory domain.
 - Instances should be managed in a BlueXP edge caching specific Organizational Unit (OU) and excluded from inherited company GPOs.
- Service account. The services on the 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 BlueXP edge caching 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 BlueXP).

License Management Server

- The BlueXP edge caching 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 BlueXP edge caching Core instance in the datacenter or cloud.

- If you require a separate BlueXP edge caching LMS instance, you need to install the latest BlueXP edge caching software installation package on a pristine Microsoft Windows Server instance.
- The LMS instance needs to be able to connect to the subscription service (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 BlueXP edge caching 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 BlueXP edge caching Edge and Core instances.
- BlueXP edge caching TCP Ports: 443 (HTTPS), 6618-6630.
- Network optimization devices (such as Riverbed Steelhead) must be configured to pass-thru BlueXP edge caching specific ports (TCP 6618-6630).

Getting started

You use BlueXP to deploy the BlueXP edge caching Management Server and Core software in the working environment.

Enable BlueXP edge caching using BlueXP

In this configuration you will deploy the BlueXP edge caching Management Server and BlueXP edge caching Core in the same working environment where you created your Cloud Volumes ONTAP system using BlueXP.

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:



Deploy Cloud Volumes ONTAP

Deploy Cloud Volumes ONTAP and configure SMB file shares. For more information, see [Launching Cloud Volumes ONTAP in Azure](#), [Launching Cloud Volumes ONTAP in AWS](#), or [Launching Cloud Volumes ONTAP in Google Cloud](#).

2

Deploy the BlueXP edge caching Management Server

Deploy an instance of the BlueXP edge caching Management Server in the same working environment as the instance of Cloud Volumes ONTAP.

3

Deploy the BlueXP edge caching Core

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

4

License BlueXP edge caching

Configure the BlueXP edge caching License Management Server (LMS) service on a BlueXP edge caching 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 BlueXP edge caching Edge instances

See [Deploying BlueXP edge caching Edge instances](#) to deploy the BlueXP edge caching Edge instances in each remote location. This step is not done using BlueXP.

Deploy Cloud Volumes ONTAP as your storage platform

BlueXP edge caching supports Cloud Volumes ONTAP deployed in Azure, AWS, and Google Cloud. For detailed prerequisites, requirements, and deployment instructions, see [Launching Cloud Volumes ONTAP in Azure](#), [Launching Cloud Volumes ONTAP in AWS](#), or [Launching Cloud Volumes ONTAP in Google Cloud](#)

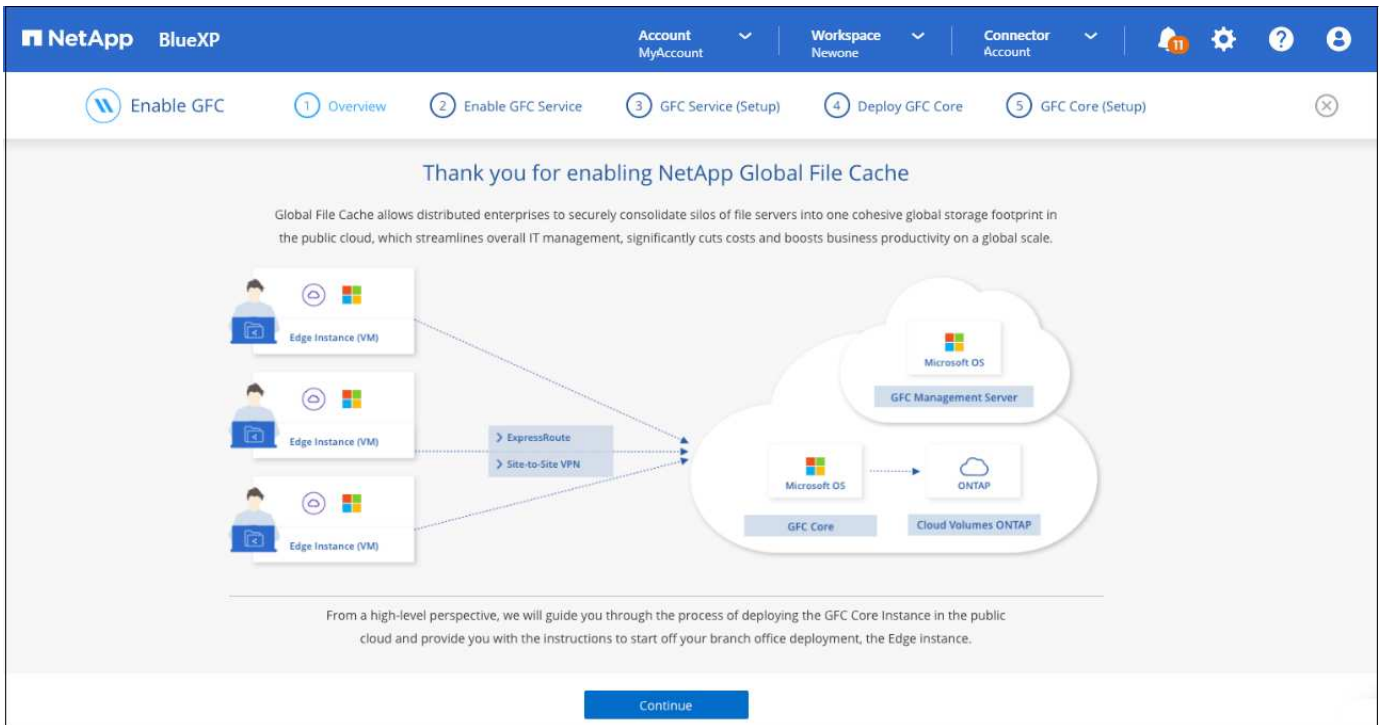
Note the following additional BlueXP edge caching requirement:

- 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 BlueXP edge caching components.

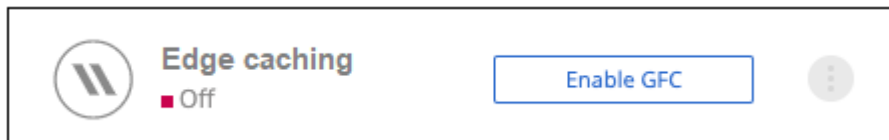
Enable BlueXP edge caching in your working environment

The installation wizard walks you through the steps to deploy the BlueXP edge caching Management Server instance and the BlueXP edge caching Core instance, as highlighted below.



Steps

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



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.

SMB Setup

SMB Server Active Directory Domain <input type="text" value="gfc.netapp.com"/> Name Server IP Address <input type="text" value="10.0.2.4"/> Active Directory Admin User <input type="text" value="cvoadmin"/> Active Directory Admin Password <input type="password" value="*****"/>	SMB Share Volume Name <input type="text" value="Enter Volume Name"/> Volume Size(GB) <input type="text"/> Select Aggregate <input type="text" value="Select Aggregate"/> Share Name <input type="text" value="Enter Share Name"/> Thin provisioning <input type="checkbox"/> Enabled ⓘ Deduplication <input type="checkbox"/> Enabled ⓘ
---	--

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.

Enable Global File Cache Service

Licensing Global File Cache:

Once you've completed this deployment process, you will need your NSS Credentials to activate your subscription. If you haven't purchased or received your NetApp Global File Cache licenses, which are available as an Edge-based license, they can be purchased through your NetApp Partner or NetApp Sales Representative.

How many edge instances are you planning to deploy?

Before you begin:

Here are the most important requirements for your environment before you can deploy the NetApp Global File Cache solution:

Configure the required Network Configuration and Firewall Rules for Global File Cache



Create a "Service Account" in your Active Directory domain: GFC.NETAPP.COM



Update Antivirus Exclusions for your Windows Server infrastructure by committing the required exclusions to your Antivirus services



For more information on all the solution requirements [Click Here](#)

Continue

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 BlueXP edge caching Management Server VM and click **Enable GFC Service**. For Azure and Google Cloud 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.

Global File Cache Service (Setup)

Information

Subscription Name	OCCM Dev
Azure Region	eastus
VNet	Vnet1
Subnet	Subnet2
Resource Group	occm_group_eastus

Credentials & Virtual Machine

Local Admin Name

Local Admin Password

VM Name

Enable GFC Service

8. After the BlueXP edge caching Management Service is successfully deployed, click **Continue**.
9. For the BlueXP edge caching Core, enter the admin user credentials to join the Active Directory domain, and the service account user credentials. Then click **Continue**.
 - The BlueXP edge caching 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.

Deploy Global File Cache Core

Active Directory and Admin Credentials

Provide administrative credentials to join the GFC Core instance to the Active Directory domain

Join Active Directory Domain ⓘ

Admin User ⓘ

Admin Password ⓘ

Account User Credentials

Provide Service Account credentials

Service Account User ⓘ

Service Account Password ⓘ

Continue

10. Enter the admin credentials you will use to access to the BlueXP edge caching Core VM and click **Deploy GFC Core**. For Azure and Google Cloud 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.

Global File Cache Core (Setup)

Information

Subscription Name	Subscription_1234567891234...
Region	East US Virginia
VNet	VNet_1234567
Subnet	10.0.0.0/24
Resource Group	Resource Group 1

Credentials & Virtual Machine

Local Admin Name

Local Admin Password

VM Name

Local Admin Name & Password are inherited from the Global File Cache Management Service. The Virtual Machine Name is associated to your Cloud Manager Account

[Deploy GFC Core](#)

11. After the BlueXP edge caching Core is successfully deployed, click **Go to Dashboard**.

Global File Cache

Global File Cache Management Instance

	www.working-environment-1.com <small>Hostname</small>	ON <small>Status</small>
141.226.210.219 <small>IP Address</small>	East US <small>Region</small>	VNet1 <small>VNet</small>
10.10.10.10/24 <small>Subnet</small>	RGName <small>Resource Group</small>	26% <small>CPU Utilization</small>

1 Working Environment

	Working Environment_1 <small>Name</small>	High Availability <small>Type</small>	ON <small>Status</small>	2 <small>Core Instances</small>	Add Core Instance
--	--	--	-----------------------------	------------------------------------	--

Instance Core 1
ON

www.working-environment-1.com <small>Hostname</small>	141.226.210.219 <small>IP Address</small>	26% <small>CPU Utilization</small>	2.5 TB <small>Network Inbound</small>	2.5 TB <small>Network Outbound</small>	Deploy GFC Edge
--	--	---------------------------------------	--	---	--

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

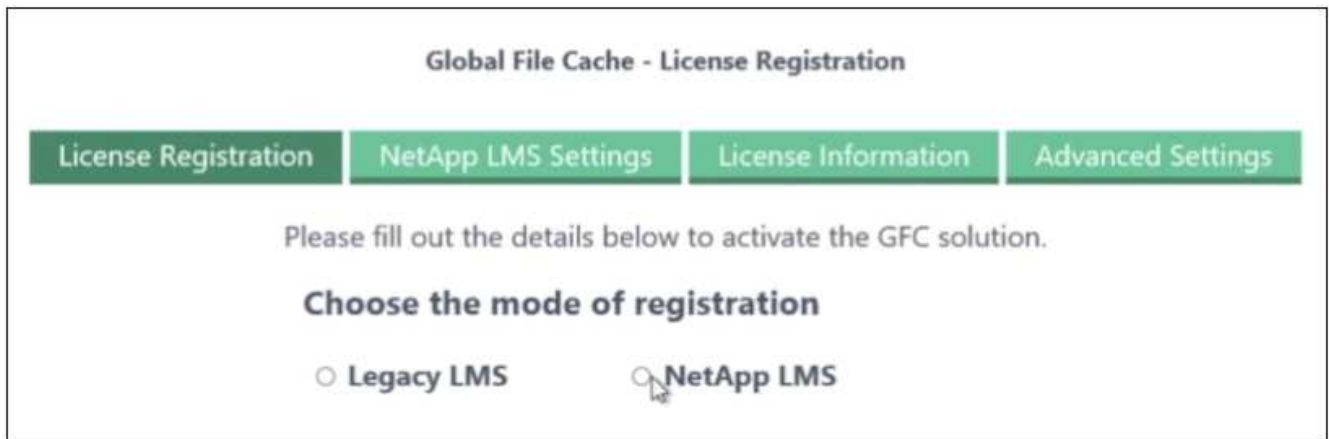
License your BlueXP edge caching installation

Before you can use BlueXP edge caching, you need to configure the BlueXP edge caching License Management Server (LMS) service on a BlueXP edge caching 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 BlueXP edge caching Core (the Core you are designating as your LMS service) using the following URL. Replace `<ip_address>` with the IP address of the BlueXP edge caching 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 BlueXP edge caching 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**.

Global File Cache - License Registration

License Registration
NetApp LMS Settings
License Information
Advanced Settings

Please fill out the details below to activate the GFC solution.

Choose the mode of registration

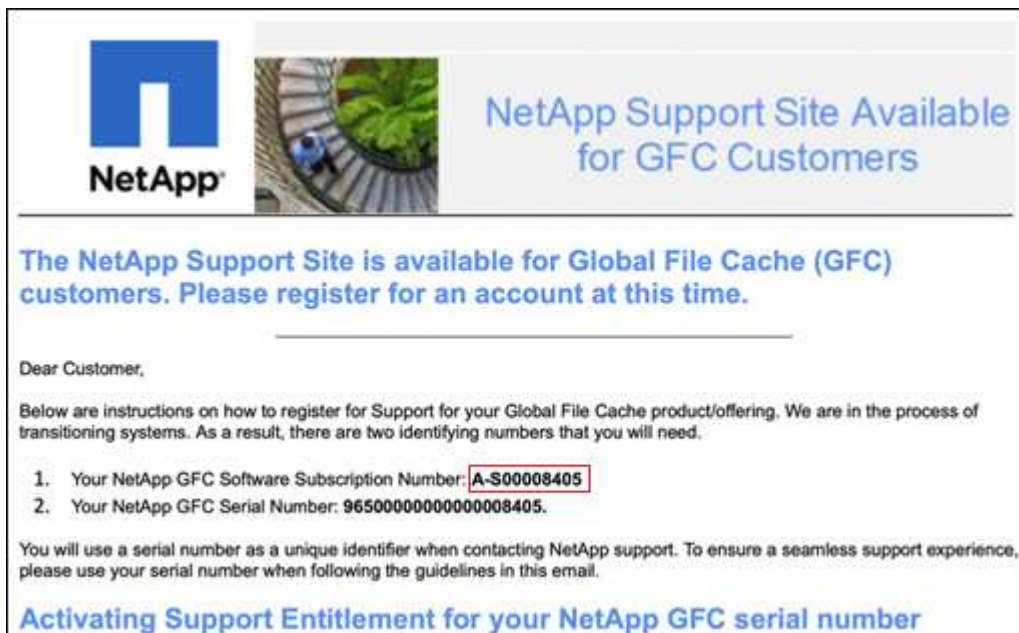
☐ Legacy LMS
☒ **NetApp LMS**

Customer Id:

* Choose a unique identifier for your GFC deployment, preferably your email address

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 BlueXP edge caching 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 BlueXP edge caching Edge instances](#) in each of your remote offices.

Deploy additional Core instances

If your configuration requires more than one BlueXP edge caching 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 BlueXP edge caching 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.

Deploy Global File Cache Core

Active Directory and Admin Credentials

Provide administrative credentials to join the GFC Core instance to the Active Directory domain

Join Active Directory Domain ⓘ

Admin User ⓘ

Admin Password ⓘ

Account User Credentials

Provide Service Account credentials

Service Account User ⓘ

Service Account Password ⓘ

Continue

3. Enter the admin credentials you will use to access to the BlueXP edge caching Core VM and click **Deploy GFC Core**. For Azure and Google Cloud 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.

Global File Cache Core (Setup)

Information

Subscription Name	Subscription_1234567891234...
Region	East US Virginia
VNet	VNet_1234567
Subnet	10.0.0.0/24
Resource Group	Resource Group 1

Credentials & Virtual Machine

Local Admin Name

Local Admin Password

VM Name

Local Admin Name & Password are inherited from the Global File Cache Management Service. The Virtual Machine Name is associated to your Cloud Manager Account

[Deploy GFC Core](#)

4. After the BlueXP edge caching Core is successfully deployed, click **Go to Dashboard**.

1 Working Environment

Working Environment_1

Name

High Availability

Type

ON

Status

2

Core Instances

Add Core Instance

Instance Core 1 | ON

www.working-environment-1.com

Hostname

141.226.210.219

IP Address

26%

CPU Utilization

2.5 TB

Network Inbound

2.5 TB

Network Outbound

Deploy GFC Edge

Instance Core 1 | ON

www.working-environment-1.com

Hostname

141.226.210.219

IP Address

26%

CPU Utilization

2.5 TB

Network Inbound

2.5 TB

Network Outbound

Deploy GFC Edge

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

Before you begin to deploy BlueXP edge caching Edge instances

There are many requirements you need to be aware of before you begin to install BlueXP edge caching Edge software in your remote offices.

Download required resources

Download the BlueXP edge caching 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 \(Microsoft Hyper-v\)](#)

- BlueXP Edge Caching Edge Software:

[NetApp GFC Software Installation Package \(.EXE\)](#)

- Global File Cache Dashboards for Cloud Insights:

[NetApp GFC Cloud Insights Dashboards \(.ZIP\)](#)

- Global File Cache Documentation:

[NetApp Global File Cache User Guide \(.PDF\)](#)

Follow [these steps](#) to upgrade your BlueXP edge caching Edge software.



When deploying BlueXP edge caching on Windows Server 2016, you should be using .NET Framework 4.8 and Windows WebView2 framework.

Designing and deploying BlueXP edge caching Edge

Depending on your requirements, you might need to deploy one or multiple 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 BlueXP edge caching Core instance. The BlueXP edge caching Edge should contain a D: \ NTFS volume, which contains the cached files within the branch office.



For the BlueXP edge caching Edge, it is important to understand the [sizing guidelines](#). This will assist you in making the correct design for your BlueXP edge caching 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.

BlueXP edge caching Edge instance

When deploying a BlueXP edge caching 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 edge caching .OVA or .VHD template, which includes the Windows Server operating system of choice and BlueXP edge caching software.

Quick steps

1. Deploy the BlueXP edge caching 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 BlueXP edge caching Edge software.
4. Identify the BlueXP edge caching Management Server and Core instance.
5. Configure the BlueXP edge caching Edge instance.

BlueXP edge caching Edge requirements

The BlueXP edge caching Edge is designed to function across all platforms supporting Windows Server 2016 and 2019, bringing simplified IT to corporate remote offices and beyond. Critically, BlueXP edge caching 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.

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

Physical hardware requirements

- Minimum 8 CPU cores
- Minimum 32 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 BlueXP edge caching, 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: 8 vCPU cores.
- Memory (RAM): Minimum: 32 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: 8 vCPU cores @ 10000 MHz.
- Memory (RAM): Minimum: Reservation of 32 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 BlueXP edge caching drives as removable.
- Networking: Network Interface must be set to **VMXNET3** (may require VM Tools).

The Edge 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 BlueXP edge caching Edge and Management Server and Core instances.

BlueXP edge caching TCP Ports: 443 (HTTPS - LMS), 6618 - 6630.

- Network optimization devices (such as Riverbed Steelhead) must be configured to pass-thru BlueXP edge caching specific ports (TCP 6618-6630).

Client workstation and application best practices

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

NetApp does not recommend the installation nor application of monitoring or antivirus solutions on any BlueXP edge caching 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 BlueXP edge caching 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:
 - The BlueXP edge caching Core instance listens on TCP ports 6618-6630, ensure that BlueXP edge caching Edge instances can connect to these TCP ports.
 - BlueXP edge caching instances require communications to the BlueXP edge caching Management Server on TCP port 443 (HTTPS).
- Network optimization solutions/devices must be configured to pass-thru BlueXP edge caching specific ports.

Antivirus best practices

NetApp has tested most commonly used antivirus products including Cylance, McAfee, Symantec, Sophos, Trend Micro, Kaspersky, Crowd Strike, Cisco AMP, Tanium, and Windows Defender for use in conjunction with BlueXP edge caching. The antivirus software should be certified by NetApp and is supported only if configured with the proper exclusion list. See Appendix A in the [NetApp Global File Cache User Guide](#)



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 BlueXP edge caching 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\GfcCIAgentService.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

BlueXP edge caching instances are designed specifically as the primary application running on a Windows Server 2016 and 2019 platform. BlueXP edge caching 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, supported services and applications on the server running BlueXP edge caching are limited to:
 - DNS/DHCP
 - Active Directory domain controller (BlueXP edge caching must be on a separate volume)
 - Print services
 - Microsoft System Center Configuration Manager (SCCM)
 - BlueXP edge caching approved client-side system agents and anti-virus applications
- NetApp Support and maintenance applies only to BlueXP edge caching.
- 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-BlueXP edge caching software which might be installed on the server running BlueXP edge caching:
 - If any third-party software package causes software or resource conflicts with BlueXP edge caching or

performance is compromised, the NetApp support organization might require the customer to disable or remove the software from the server running BlueXP edge caching.

- It is the customer's responsibility for all installation, integration, support, and upgrade of any software added to the server running the BlueXP edge caching 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 BlueXP edge caching 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 BlueXP edge caching or performance is compromised, there might be a requirement by BlueXP edge caching's support organization to disable/remove the software.

Deploy BlueXP edge caching Edge instances

After you have verified that your environment meets all the requirements, you install BlueXP edge caching Edge software in each remote office.

Before you begin

To complete BlueXP edge caching Edge configuration tasks, you need the following information:

- Static IP addresses for each BlueXP edge caching instance
- Subnet mask
- Gateway IP address
- The FQDN you wish to assign to each BlueXP edge caching 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 BlueXP edge caching 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:

- BlueXP edge caching Licensing TCP Port: 443
- BlueXP edge caching TCP Ports: 6618-6630

Deploy the BlueXP edge caching Virtual Template

The virtual template (.OVA and .VHD) images contain the latest release of the BlueXP edge caching software. If you are deploying BlueXP edge caching 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 installation of the BlueXP edge caching 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 BlueXP edge caching Edge configuration section.

Configure the BlueXP edge caching Edge instance

The BlueXP edge caching Edge instance connects to a BlueXP edge caching 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 BlueXP edge caching 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 BlueXP edge caching 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 BlueXP edge caching 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.

- Click **Add** to confirm the addition of the BlueXP edge caching Core appliance. A confirmation box will appear. Click **OK** to dismiss it.

The screenshot shows the NetApp Global File Cache Configuration Console. The top navigation bar includes 'System Overview', 'System Configuration', 'GFC Configuration', and 'Policy Configuration'. The 'GFC Configuration' tab is active, with sub-tabs for 'GFC Core' and 'GFC Edge'. The left sidebar lists sections: 'Section', 'Core Instances', 'Pre-Population', 'Advanced Options', 'Throttling', and 'Cache Cleaner'. The main content area is titled 'Core Instances' and contains the following configuration options:

- Core Auto Configuration** (checkbox, unchecked) (Requires License Manager Server)
- Associate this Edge instance with a Core**
- Cloud Fabric ID** (text input)
- FQDN / IP Address** (text input)
- Enabled SSL** (checkbox, unchecked)
- User Name** (text input) (Optional)
- Password** (text input) (Optional)
- Add** button

Below these fields is a table with the following data:

Cloud Fabric ID	FQDN/IP Address	SSL Enabled
<input type="checkbox"/> NLAMS	192.168.1.213	0

At the bottom right of the table is a **Delete** button.

Update BlueXP edge caching Edge software

BlueXP edge caching 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 BlueXP edge caching software, it is possible that a newer version is available on the NetApp Support Download portal.

Ensure that your BlueXP edge caching 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 BlueXP edge caching installation package:

Steps

- After saving the latest installation package to the desired Windows Server instance, double-click it to run the installation executable.
- Click **Next** to continue the process.
- Click **Next** to continue.
- Accept the Licensing Agreement and click **Next**.
- 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](#).

Copyright information

Copyright © 2024 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.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

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.