NetApp Global File Cache 1.0

User Guide

NetApp

Important: If you are using Cloud Manager to enable Global File Cache, you should use https://docs.netapp.com/us-en/occm/concept_gfc.html for a step-by-step walkthrough.

Cloud Manager automatically provisions the GFC Management Server instance alongside the GFC Core instance and enables entitlement / licensing.

You can still use this guide as a reference. Chapter 7 through 13 contains in-depth information and advanced configuration parameters for GFC Core and GFC Edge instances.

Additionally, this document includes overall onboarding and application best practices.

© 2020 NetApp, Inc. All Rights Reserved.

TABLE OF CONTENTS

1 Introduction 8

1.1 The GFC Fabric: Highly Scalable and Flexible 8

1.2 Next Generation Software-Defined Storage 8

1.3 Global File Cache Software 8

1.4 Enabling Global File Cache using NetApp Cloud Manager 8

2 NetApp Global File Cache Requirements 9

2.1 Hardened Server Appliance 9

2.2 Physical Hardware Requirements 9

2.3 Virtual Deployment Requirements (i.e. Microsoft Hyper-V or VMware vSphere) 9

2.4 Cloud Deployments (such as Microsoft Azure, Google Cloud Platform or Amazon AWS) 10

2.5 Operating System/Software Requirements 10

2.6 Backend File Server Requirements 11

2.7 Partition Sizing Requirements 11

2.8 GFC Intelligent File Cache Disk Requirements (D:\) 11

2.9 Networking 12

2.10 Networking (External Access) 12

2.11 Client Workstation Settings 12

2.12 NetApp Support Policy 13

2.13 Firewall and Antivirus Best Practices 14

3 Getting Started with NetApp Global File Cache 17

3.1 Example: Deployment Summary 17

3.2 Example: Centralized Data Store in the On prem, hybrid or public cloud 18

3.3 GFC Fabric 19

3.4 Sizing Guidelines 19

4 Deploying NetApp Global File Cache Virtual Template and Software Package 21

4.1 Before You Begin 21

4.2 Deploying the GFC Virtual Template 21

4.3 Network Configuration 22

4.4 Active Directory Configuration 24

4.5 Software Installation Package (Update) 26

5 Licensing 28

5.1 How It Works 28

5.2 Subscription Updates 28

© 2020 NetApp, Inc. All Rights Reserved.

5.3 Caching 28
5.4 Requirements 28
5.5 Deploying GFC LMS instance 28

6 Initial Configuration 32

6.1 Initial Configuration Wizard 32
6.2 Talon Configuration Console 33

7 Designing and Deploying NetApp Global File Cache Core 36

7.1 GFC Core Stand-Alone Instance 36
7.2 GFC Core Load Distributed Design 36
7.3 Configuring GFC Core instance – Service Account 37
7.4 Configuring GFC Core instance – Backend File Servers 37
7.5 GFC Core Advanced Features 39
7.6 Global Exclusion List 39
7.7 Server Exclusion List 39
7.8 Remote Inclusion List 40
7.9 Selectable File Handling 41
7.10 Core Pre-population 42
7.11 Core Advanced Options 45

8 Designing and Deploying NetApp Global File Cache Edge 47

8.1 GFC stand-alone instance 47
8.2 GFC Edge Multi-Edge Deployment 47
8.3 Configuring the GFC Edge Role 52
8.4 GFC Edge Advanced Features 53

9 DFS Namespace Integration 57

9.1 DFS Design 57
9.2 Site Definitions and Site Links 57
9.3 DFS Root Configuration Default 59
9.4 Site Costing Configuration 62
9.5 GFC Global Exclusion Configuration (DFS) 63

10 Central Monitoring using Microsoft SCOM 65

10.1 Deploying GFC SCOM Management Pack 65
10.2 Dashboards and Reports 67
10.3 Personalized Views 67
10.4 Core Instances 68

© 2020 NetApp, Inc. All Rights Reserved.

10.5 Edge Instances ... 71
10.6 Where do I Find? ... 74
10.7 Event Analysis ... 75
10.8 Log Analysis ... 75

11 Client Application Best Practices ... 78

11.1 Autodesk - Revit ... 78
11.2 Revit Best Practices Summary ... 80
11.3 Autodesk - AutoCAD ... 81
11.4 Bentley – MicroStation ... 84
11.5 Adobe Creative Suite ... 86
11.6 Mac OSX Best Practices (10.12 Onwards) ... 87

12 End User Training ... 91

Accessing Project Folders and Files ... 91
Cold Files Versus Warm Files ... 91
Do's and Don'ts ... 91
Application-Specific Best Practices ... 92

13 Contact Details ... 92

Appendix A: Antivirus Application Suites ... 93

McAfee VirusScan ... 93
McAfee VirusScan - Central Management Console ... 101
Symantec Endpoint Protection 12.x ... 104
Sophos Endpoint Security and Control v10.x ... 111
Trend Micro Officescan ... 116
Kaspersky Endpoint Security Cloud ... 118
Windows Defender ... 120

Appendix B: Disable VMware ESX(i) Hot Plug Capability ... 123

To Disable HotPlug Capability Using the vSphere Client ... 123
To Disable HotPlug Capability Using the vSphere Web Client ... 123
To Disable HotPlug Capability by Editing the Virtual Machine's .vmx File ... 123

Appendix C: NetApp Global File Cache (GFC) PowerShell Configuration ... 124

GFC Optimus PSM ... 124
Configuration Process ... 124
GFC Namespace for TUMMIProvider ... 138

© 2020 NetApp, Inc. All Rights Reserved.

§Appendix D: NetApp Global File Cache Event ID / Logging / 3rd Party Monitoring 148
NetApp Global File Cache Event IDs 148
GFC Logging 149
GFC File Transfer Summary Logging 150
GFC Processes / Services 150
Where to Find Additional Information 151

© 2020 NetApp, Inc. All Rights Reserved.

© 2020 NetApp, Inc. All Rights Reserved.

1 Introduction

Welcome to the NetApp Global File Cache User Guide. This manual will assist you in designing, deploying, managing, and maintaining your NetApp Global File Cache (GFC) infrastructure. The next few pages will provide a brief introduction and overview of GFC, and how it can be leveraged to enable data centralization, cloud storage consolidation, global file-sharing, and collaboration for distributed enterprises.

GFC allows businesses to centralize data, leveraging customer's on prem, hybrid or public cloud storage infrastructure, while consolidating distributed storage and IT assets. The software extends to users globally, providing real-time global file-sharing and collaboration to end users.

1.1 The GFC Fabric: Highly Scalable and Flexible

GFC transparently fits any IT environment, as the solution is storage cloud platform agnostic, supporting on prem NetApp Data ONTAP (AFF / FAS), Cloud Volumes ONTAP, Cloud Volumes Service or Azure NetApp Files. Whether you want to leverage Microsoft Azure, Google Cloud Platform or Amazon Web Service public cloud storage infrastructure, GFC immediately extends the value of your central storage to your distributed locations.

In a nutshell, GFC creates an intelligent file caching software appliance at each distributed location, running on Microsoft Windows Server. The software overlays the Microsoft Windows File-Sharing mechanism, fully integrating with the Microsoft security principles like Active Directory, ACLs, and NTFS permissions, and allows it to work at a global scale, even in locations with low bandwidth or high latency.

1.2 Next Generation Software-Defined Storage

- GFC runs on Microsoft Windows Server 2016 and 2019.
- Fully integrates with customer's Microsoft ecosystem.
  (AD DS, DNS/DHCP, Print Services, SCCM, SCOM, PowerShell).
- Available as software installation package or virtual appliance template.

1.3 Global File Cache Software

- Flexible: Storage agnostic, works with SMB/CIFS infrastructure, including NetApp Data ONTAP, Cloud Volumes ONTAP, Cloud Volumes Service or Azure NetApp Files.
- Intelligent: Caches only what's needed at the branch (active dataset).
- Zero-touch: Automatically purges stale cached files over time (LRU).
- Performant: Compresses, streams, and reduces data.
- Consistent: Central file-locking for enterprise applications.

Important: This guide is designed for MANUAL deployment and enablement of the GFC solution.

For more information, including quick-start videos on the deployment of Global File Cache, visit: https://cloud.netapp.com/global-file-cache/onboarding

1.4 Enabling Global File Cache using NetApp Cloud Manager

For enablement of Global File Cache through Cloud Manager, please consult the following page for a step-by-step walkthrough: https://docs.netapp.com/us-en/occm/concept_gfc.html

© 2020 NetApp, Inc. All Rights Reserved.

2 NetApp Global File Cache Requirements

NetApp Global File Cache (GFC) is cloud platform agnostic, and specifically designed to function across all platforms supporting Windows Server 2016 and 2019, bringing simplified IT to corporate distributed branch offices and beyond. Critically, GFC can be deployed on customers' existing hardware infrastructure, virtualization, or on prem, hybrid or public cloud environments in almost every case if they meet a few base-level requirements.

GFC requires the following hardware and software resources to function optimally. For more information about overall sizing guidelines, please consult Section 3 of this user guide.

2.1 Hardened Server Appliance

The GFC installation package creates a hardened software appliance on any Microsoft Windows Server instance. **DO NOT UNINSTALL THE GFC PACKAGE**. Uninstalling GFC will impact the functionality of the server instance and may require a full rebuild of the server instance. *** IMPORTANT**

2.2 Physical Hardware Requirements

- Minimum 4 CPU Cores.
- Minimum 16GB RAM.
- Dedicated Single or Redundant 1Gbps NIC.
- 10k RPM SAS HDD or SSD (preferred).
- RAID controller with write-back caching functionality enabled *** IMPORTANT.**

2.3 Virtual Deployment Requirements (i.e. Microsoft Hyper-V or VMware vSphere)

Note: Hypervisor platforms are known to be subject to performance degradation from a storage subsystem perspective (e.g. latency). For optimal performance using GFC, 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 onwards

- **Processor (CPU):** CPUs must be set as Static: Minimum: 4vCPU Cores.
- **Memory (RAM):** Minimum: 16GB set as Static.
- **Hard Disk Provisioning:** Hard Disks must be configured as “Fixed Disk”.

VMware vSphere 6.x onwards

- **Processor (CPU)** * IMPORTANT: Reservation of CPU Cycles must be set. Minimum: 4 vCPU Cores @ 10000MHz.
- **Memory (RAM)** * IMPORTANT: Minimum: Reservation of 16GB.
- **Hard Disk Provisioning** * IMPORTANT:

Disk Provisioning set as “Thick Provisioned Eager Zeroed”,

Hard Disk Shares set to High,

Set “devices.hotplug” to “false” using the vSphere Client to prevent Microsoft Windows from presenting GFC drives as “removable”.

See Appendix B for the steps to apply this setting

- **Networking** * IMPORTANT: Network Interface needs to be set to VMXNET3 (requires VMTools).

© 2020 NetApp, Inc. All Rights Reserved.

Note: GFC 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 virtual machine's guest operating system and management of the virtual machine, such as VMTools.

2.4 Cloud Deployments (such as Microsoft Azure, Google Cloud Platform or Amazon AWS)

For best performance in public cloud environments, the following requirements must be met:

Public Cloud Deployments

- Microsoft Azure

Standard D Series (i.e. D4s_v3) or equivalent

Minimum: 4 vCPU / 16GB RAM

See also: https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes-general

- Amazon AWS (EC2)

M/C Instance Type (i.e. m4.xlarge) or equivalent

Minimum: 4 vCPU/16GB RAM

See also: https://aws.amazon.com/ec2/instance-types/

2.5 Operating System/Software Requirements

- Windows Server 2016 Standard/Datacenter or Windows Server 2019 Standard/Datacenter.
- Latest Microsoft updates should be installed to ensure optimal stability, performance, and security.
- GFC server base deployment requirements:

Administrative Privileges (Domain Administrator),

A unique (geographical) NetBIOS name for the instance (i.e. NYC-FAST1),

IP Address, Subnet Mask, Gateway Address, and DNS Server details,

Active Directory Domain name.

- GFC instances should be joined to the customer's Active Directory domain.
- GFC instances should be managed in a GFC-specific OU (Organizational Unit) and excluded from inherited company GPO's.
- Service Account: Username and Password for a domain user that has backup/restore privileges.

Service Account should be configured with the following account options:

User must change password at next logon = DISABLED (unchecked),

Password never expires = ENABLED (checked).

- GFC instances must be on the same VLAN as the datacenter backend storage infrastructure (1 hop).

This service account user must be a member of the "Backup Operators" group on Windows datacenter file servers and when using Azure NetApp Files.

© 2020 NetApp, Inc. All Rights Reserved.

Global File Cache Service Account & Azure NetApp Files

You can include additional accounts that require elevated privileges to the computer account created for use with Azure NetApp Files. The specified accounts will be allowed to change the NTFS permissions at the file or folder level. For example, you can specify a non-privileged service account used for migrating data to an SMB file share in Azure NetApp Files.

Please consult https://docs.microsoft.com/en-us/azure/azure-netapp-files/azure-netapp-files-create-volumes-smb to enable the ***"ANFBackupOperator"*** feature and add the Global File Cache service account to the Azure NetApp Files ***"Backup Policy Users"*** list.

Global File Cache Service Account on other platforms

This service account user must be a member of the local "Administrator" group on storage platforms like ONTAP, Cloud Volumes ONTAP or Cloud Volumes Service.

2.6 Backend File Server Requirements

- Backend storage platform should present SMB File shares, Azure NetApp Files Shares, or iSCSI/FC Interface.
- Backend storage platform should support NTFS File System, ACLs, and Local SAM Database when leveraging a Non-Windows SMB interface.
- Network Latency between GFC and backend file storage should be < 1ms.
- **Important: Most storage tiering systems do not meet this requirement / SLA.**

2.7 Partition Sizing Requirements

- C:\ Minimum 250 GB (System/Boot Volume).
- D:\ Minimum 1 TB (Separate Data Volume for GFC 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. A cache volume is not required on Cores as Cores do not cache data.

2.8 GFC Intelligent File Cache Disk Requirements (D:\)

Disk Latency should deliver < 0.5ms average IO Disk latency and 1MiB/sec throughput **per concurrent user**.

- Download the DiskSpd tool from Microsoft to confirm storage performance on the GFC instance:

https://gallery.technet.microsoft.com/DiskSpd-A-Robust-Storage-6ef84e62

- Perform the following command on D:\ (Cache Volume) to confirm

Diskspd.exe -b8K -d60 -L -o2 -t4 -r -w30 -c500M D:\io.dat > results.txt

Confirm the results in results.txt

Total Read IO AvgLat should be < 0.500 ms

Total Write IO AvgLat should be < 0.500 ms

Write MiB/s should be 1MiB/s per user, i.e. for 100 concurrent sessions the Total Write MiB/s should be > 100 MiB/s

- Example Result:

```
Read IO
thread |       bytes     |     I/Os     |    MiB/s   |  I/O per s |  AvgLat  | LatStdDev |  file
```


© 2020 NetApp, Inc. All Rights Reserved.

```
------------------------------------------------------------------------------------------------------
     0 |      3608035328 |       440434 |      57.34 |    7340.13 |    0.242 |     1.912 |
D:\io.dat (500MiB)
     1 |      3857448960 |       470880 |      61.31 |    7847.54 |    0.227 |     1.805 |
D:\io.dat (500MiB)
     2 |      3631136768 |       443254 |      57.71 |    7387.13 |    0.241 |     1.941 |
D:\io.dat (500MiB)
     3 |      3721641984 |       454302 |      59.15 |    7571.25 |    0.234 |     1.882 |
D:\io.dat (500MiB)
------------------------------------------------------------------------------------------------------
total:       14818263040 |      1808870 |     235.52 |   30146.06 |    0.236 |     1.884

Write IO
thread |       bytes     |     I/Os     |    MiB/s   |  I/O per s |  AvgLat  | LatStdDev |  file
------------------------------------------------------------------------------------------------------
     0 |      1546100736 |       188733 |      24.57 |    3145.36 |    0.066 |     0.933 |
D:\io.dat (500MiB)
     1 |      1655848960 |       202130 |      26.32 |    3368.63 |    0.060 |     0.651 |
D:\io.dat (500MiB)
     2 |      1559379968 |       190354 |      24.78 |    3172.38 |    0.064 |     0.794 |
D:\io.dat (500MiB)
     3 |      1598201856 |       195093 |      25.40 |    3251.36 |    0.065 |     0.821 |
D:\io.dat (500MiB)
------------------------------------------------------------------------------------------------------
total:        6359531520 |       776310 |     101.08 |   12937.74 |    0.064 |     0.804
```

2.9 Networking

- Firewall: TCP ports should be allowed between GFC edge and core instance.
- GFC TCP Ports: 443 (HTTPS - LMS), 6618 – 6630.
- Network optimization devices (i.e. Riverbed Steelhead) must be configured to “Pass-thru” GFC-specific ports (TCP 6618-6630).

2.10 Networking (External Access)

GFC License Management Server requires external access over HTTPS (TCP port 443) to these URLs:

https://talonazuremicroservices.azurewebsites.net

https://talonlicensing.table.core.windows.net

2.11 Client Workstation Settings

GFC transparently integrates into customer’s environments, allowing users to access centralized data using their client workstations, running enterprise applications. Using GFC, data is accessed through a direct drive mapping or through a DFS namespace. For more information about the GFC Fabric, Intelligent File Caching, and key aspects of the software, consult the Getting Started with NetApp Global File Cache section of this user guide.

To ensure an optimal experience and performance, it is important to comply with the Microsoft Windows Client requirements and best practices outlined below. This applies to all versions of Microsoft Windows.

Disable Offline Files and Folders When Using Multi-Path DFS Namespaces or Collaboration Data

To ensure data integrity, Offline Files and Folders (Sync Center) should be disabled on all client workstations. This can be accomplished through a registry setting or GPO that applies to Windows clients in the environment.

- **Registry**

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CSC

Specify the **Start** value to “4”

© 2020 NetApp, Inc. All Rights Reserved.

- **Group Policy**

a. Launch Group Policy Management console from Active Directory Users and Computers
b. Navigate to the Domain policy or a specific policy that applies to Microsoft Windows Clients in your environment.
c. Select User Configuration, expand Policies, expand Administrative Templates, expand System, and expand Folder Redirection.
d. Right-click "**Do not automatically make all redirected folders available offline**" and click **Edit**.
e. Click Enabled, followed by OK.

Depending on your environmental requirements (optional):

1. Right-click "**Do not automatically make specific redirected folders available offline**" window appears.
2. Click Enabled
3. In the Options pane, select the folders that should not be made available offline by selecting the appropriate check boxes
4. Click Enabled, followed by OK

Reference: https://technet.microsoft.com/en-us/library/jj154097(v=ws.11).aspx

Microsoft Updates and Critical Patches

GFC diligently conducts QA testing and Microsoft patch validation within a week after initial release by Microsoft. It is highly recommended to test deployment of Microsoft Updates and Critical Patches after a week. Ideally, it would be recommended to roll out the updates to a test or single production instance to confirm successful deployment, before updating all GFC instances in the environment.

2.12 NetApp Support Policy

GFC instances are designed specifically for GFC as the primary application running on a Windows Server 2016 and 2019 platform. GFC requires priority access to platform resources, e.g. 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 GFC, supported services and applications on the server running GFC are limited to:

  DNS/DHCP.

  Active Directory Domain Controller (GFC cache must be on a separate volume).

  Print Services.

  Microsoft System Center Configuration Manager (SCCM).

  GFC-approved client-side system agents & anti-virus applications.
- NetApp Support and maintenance applies only to GFC.
- "Line of Business" productivity software which are typically resource intensive, e.g. database servers, mail servers, etc. are not supported.
- The customer is responsible for any non-GFC software which may be installed on the server running GFC.

If any third-party software package causes software or resource conflicts with GFC or performance is compromised, GFC's support organization may require the customer to disable or remove the software from the server running GFC.

It will be the customer's responsibility for all installation, integration, support and upgrade of any software added to the server running the GFC application.

© 2020 NetApp, Inc. All Rights Reserved.

- Systems management utilities/agents such as anti-virus tools and licensing agents may be able to coexist. However, except for the supported services and applications listed above, these applications are not supported by GFC and the same guidelines as above must still be followed.

It will be 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 GFC or performance is compromised, there may be a requirement by GFC's support organization to disable/remove the software.

2.13 Firewall and Antivirus Best Practices

Note: While GFC makes a reasonable effort to validate that the most common antivirus application suites are compatible with GFC, we cannot guarantee and are not responsible for any incompatibilities or performance issues caused by these programs, or their associated updates, service packs, or modifications.

GFC does not recommend the installation nor application of monitoring or antivirus solutions on any GFC enabled instance (Core or Edge). Should a solution be installed, by choice or by policy, the following best practices and recommendations must be applied (See Appendix A for common antivirus suites).

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 GFC Core or Edge instances.

Recommendation: Leave Microsoft Firewall settings and services at the default setting of ON, and started for Core or Edge instances that also run the Domain Controller role.

- Corporate Firewall

GFC core instance listens on TCP ports 6618-6630, ensure that GFC edge instances can connect to these TCP ports.

GFC instances require communications to the License Management Server (LMS) on TCP port 443 (HTTPS).

- Network Optimization solutions/devices must be configured to "Pass-thru" GFC-specific ports.

Antivirus Best Practices

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

Note: Adding antivirus to an Edge appliance may introduce a 10-20% impact on user performance.

Pre-Installation Notes

- The antivirus software should be certified by GFC (See appendix A).
- Individual Antivirus applications are supported when configured with proper exclusions.
- Full security suites are not supported.

© 2020 NetApp, Inc. All Rights Reserved.

Restrict File Scanning

Applications that scan files and/or folders in order to gather statistics or other data sometimes only read metadata of the file without reading actual data contained within the file. Other applications may open each file individually to determine the type of data present in the file. In the case of pictures, music, or video files, certain applications may also create thumbnails or provide additional information about the contents of the file.

Scans that cause these types of file open operations should be avoided on the edge instance and on the client workstation. Any open of a file in this manner will cause the Edge instance to retrieve the file from the backend data center file server and cache it locally in the branch office. Scanning to gather statistics or provide thumbnails to picture files could also cause the Edge instance to retrieve and cache more data than the cache was originally sized to accommodate. Client-side software that searches, indexes, and/or scans network files and folders can cause unnecessary metadata and file transfers over the WAN, resulting in an additional load on the instance and should be avoided.

Antivirus Coverage Recommendation

Antivirus software installed on the backend data center file server and on client PCs is generally adequate protection against network viruses. GFC does allow data on its Edge and Core instances to be scanned, ensuring complete point-to-point protection.

However, on both Cores and Edges, the D:\ (cache drive) volume should be excluded from virus scanning as well as any GFC processes. Users' mapped network drives should never be scanned.

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 GFC 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\tfs.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\*`

© 2020 NetApp, Inc. All Rights Reserved.

© 2020 NetApp, Inc. All Rights Reserved.

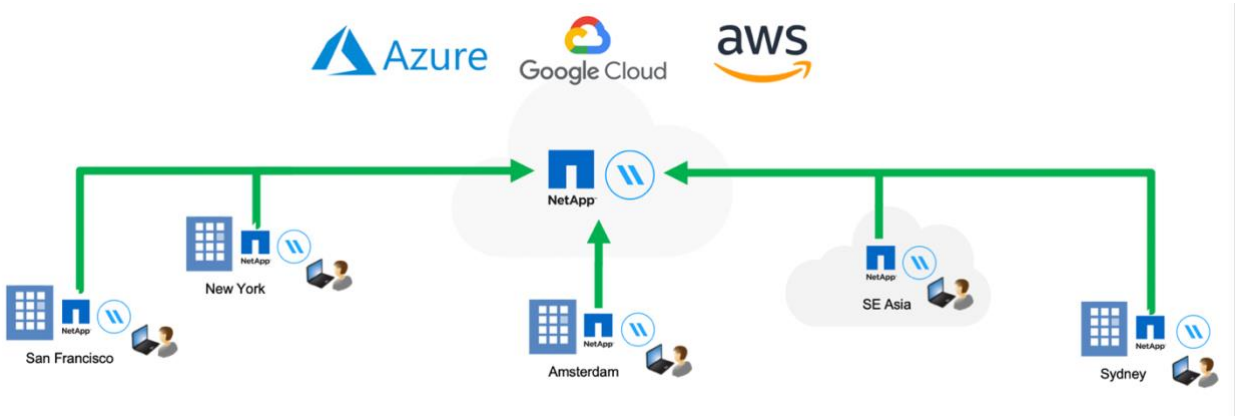
3 Getting Started with NetApp Global File Cache

NetApp Global File Cache (GFC) can be deployed in various ways, either on physical hardware or on virtualization platforms including Microsoft Hyper-V, VMware, or others. Depending on the client's needs, the software can be architected as a hub-and-spoke, symmetric, or hybrid deployment, which means that you can extend central file shares to multiple branch offices, allow branch offices to access file storage in both locations or a combination of both.

Typically, customers choose to centralize their data into one or multiple datacenters, which allows them to architect a so-called hub-and-spoke deployment. This means that all distributed locations can access centralized file storage, using the GFC Fabric, in real-time with the benefits of distributed file-locking.

Customers drive value from GFC by centralizing data and consolidating file storage from distributed branch offices into the on prem, hybrid or public cloud datacenter, i.e. Microsoft Azure, Google Cloud Platform, or Amazon Web Services.

Figure 1)



3.1 Example: Deployment Summary

The topology referenced in this example is a "hub and spoke" model, whereby the network of distributed offices/locations are all accessing one common set of data in the customer's datacenter. The key points of this example reference architecture are:

- Centralized data store: Enterprise storage in customer's on prem, hybrid or public cloud datacenter.
- GFC Fabric: Extension of the central data store to the distributed locations.
  - GFC Core Instance, mounting to corporate file shares (SMB).
  - GFC Edge Instance running in each distributed location.
  - Presents a Virtual File Share that provides access to central data.
  - Hosts the Intelligent File Cache on a custom-sized NTFS volume (D:\).
- Network configuration
  - MPLS, Virtual Private Network (VPN) connectivity or Public Internet (SSL).
- Integration with customer's Active Directory Domain Services.
- DFS-Namespace for the use of a global namespace (recommended).

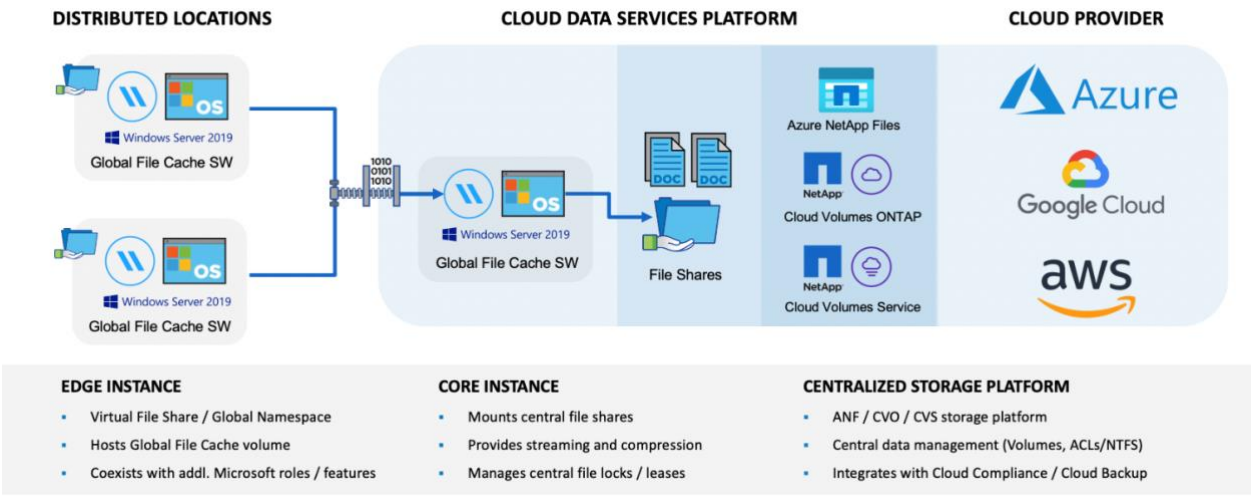
© 2020 NetApp, Inc. All Rights Reserved.

3.2 Example: Centralized Data Store in the On prem, hybrid or public cloud

The main repository for the unstructured data is a share (or number of shares) configured on the customer's on prem, hybrid or public cloud storage platform (Cloud Volumes ONTAP, Cloud Volumes Service or Azure NetApp Files) leveraging SMB integration, or by presenting a local volume associated with an iSCSI target.

The customer's cloud storage platform solution provides volumes associated with corporate file shares hosted in the on prem, hybrid or public cloud.

Figure 2) Global File Cache: Cloud Platform Agnostic



This traditional approach to storage management enables organizations to scale storage area networks (SAN) and network-attached storage (NAS) with on-demand storage, providing a familiar solution for file capacity expansion, offsite storage, and data archiving.

Presenting data in a modernized storage model allows users to work with their applications in a non-disruptive manner. All the data you put into the centralized storage solution, whether primary, file, backup, or archive, is completely under your control, and integrates with your desired platforms, backups, RTO/RPO, and BCDR strategy.

Cloud Storage Platform

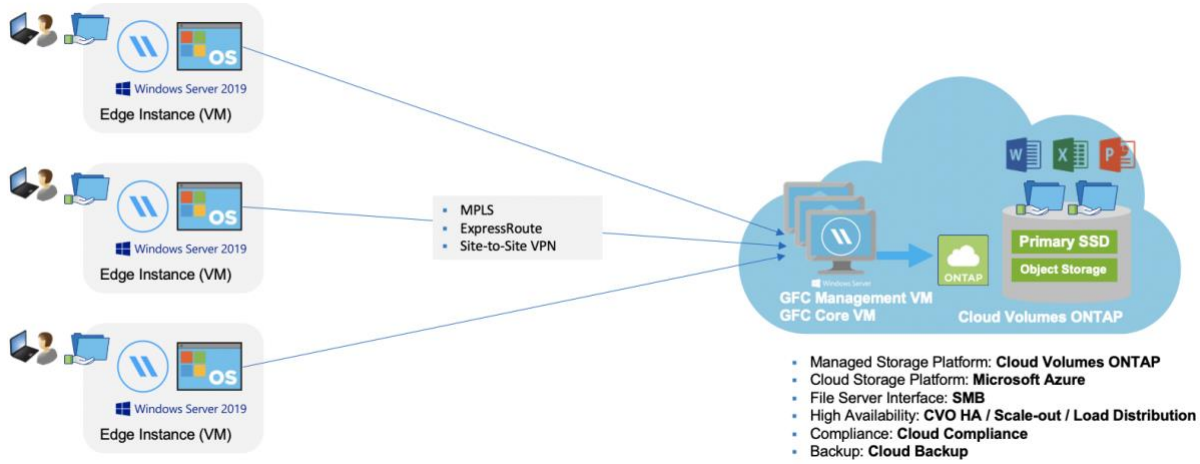
- Provides transparent SMB utilization presented by Azure NetApp Files, Cloud Volumes ONTAP or Cloud Volumes Service.
- Centralized data management (Volumes, ACLs, NTFS Permissions).
- Integrates with enterprise backup solutions (RTO/RPO).

© 2020 NetApp, Inc. All Rights Reserved.

3.3 GFC Fabric

By introducing GFC, integrating the GFC Fabric with Cloud Volumes ONTAP, Cloud Volumes Service or Azure NetApp Files, all distributed locations can use the central file storage resources as if they were local. The result is a single, centralized storage footprint, versus a distributed storage architecture that requires local data management, backup, security management, storage, and infrastructure footprint, etc. in each location.

Figure 3) Example of GFC with Cloud Volumes ONTAP in Microsoft Azure



The GFC Edge instances transparently integrate with the GFC Fabric at the customer's cloud datacenter:

- Distributed locations connect to cloud datacenter via the GFC Fabric.
- Software provides a Virtual File Share and Intelligent File Cache at each location.
  Virtual File Share is available as
  `\\Edge\FASTData\[datacenter]\[fileserver]\[share]\[folder]\`
  Access our data through DFS Namespace (recommended) or Drive Mapping.
  Intelligent File Cache can be sized based on the customer's active data set (see product requirements).
- Enables high performance global file sharing with real-time distributed file-locking.

3.4 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:

- GFC Edges/Core Ratio
- Distributed Users/GFC Edge Ratio
- Distributed Users/GFC Core Ratio

Number of Edge instances per Core instance

Our guidelines recommend up to 10 edge instances per GFC core instance, with a maximum of 20 edges per GFC 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 than 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.

© 2020 NetApp, Inc. All Rights Reserved.

Note: You can leverage multiple GFC Edge and Core instances simultaneously to scale out your infrastructure depending on the requirements. Multiple Core instances for a single set of user data is not supported when deployed using Cloud Manager at this time.

Number of concurrent users per Edge instance

The GFC Edge handles the "heavy lifting" in terms of caching algorithms and file-level differencing. A single GFC Edge instance can serve up to 400 users per physical dedicated GFC Edge instance, and up to 200 users for dedicated virtual machine 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 GFC 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 GFC Edge upper boundary (depending on physical or virtual deployment).

Note: GFC 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 GFC 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 GFC Solutions Engineer to discuss the best options for your enterprise deployment

© 2020 NetApp, Inc. All Rights Reserved.

4 Deploying NetApp Global File Cache Virtual Template and Software Package

4.1 Before You Begin

- Download the NetApp Global File Cache (GFC) Virtual Template(s) and Software Installation Packages from:

http://www.talonstorage.com/support/downloads (needs registration).

To complete basic GFC configuration tasks, you will need the following information:

Static IP addresses for each GFC instance.

Subnet Mask.

Gateway IP address.

The FQDN you wish to assign to each GFC server.

The DNS suffix (optional).

The user name and password of an administrative user in the domain.

- GFC Core instances only:

The domain name, username and password of the Service Account.

The FQDN server name of data center file servers.

- GFC Edge instances only:

The FQDN and/or IP address of the associated Core server(s).

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 GFC services. It is mandatory the devices can communicate on these ports and they be excluded from any WAN Optimization devices or Firewall restriction policies.

GFC LMS and LMC Licensing TCP Port: 44.3

GFC TCP Ports: 6618-6630.

4.2 Deploying the GFC Virtual Template

If you are deploying GFC using the .OVA or .VHD virtual machine template, follow the steps as outlined in this section. In this document we assume that you understand how to deploy the .OVA or .VHD template on the designated hypervisor platform.

Note: Ensure that virtual machine preferences, including resource reservations, are in line with the requirements as outlined in section 2: **"Virtual Deployment Requirements (i.e. Microsoft Hyper-V or VMware vSphere)"**.

Once the Virtual Template has been deployed, and virtual machine settings have been configured, feel free to start the Virtual Machine.

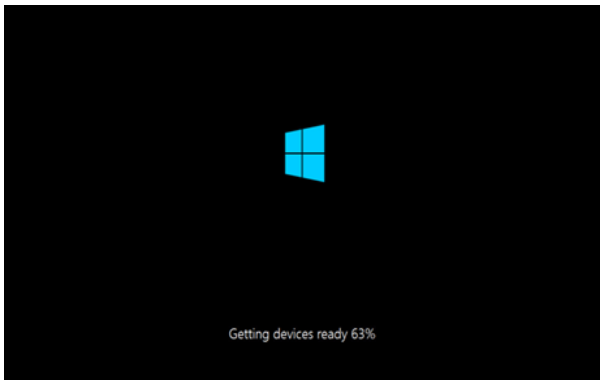
During initial boot, when the Windows Server 2016 or 2019 operating system is preparing for first use, complete the out-of-the-box experience by installing the correct drivers and installing the necessary components for the respective hardware.

When the base install of the GFC virtual 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.

Once the initial configuration wizard has completed, log in locally to the Windows Server 2016 or 2019 operating system with the following credentials:

© 2020 NetApp, Inc. All Rights Reserved.

Figure 4)



Login Credentials

Username: FASTAdmin

Password: Tal0nFAST!

Figure 5)

4.3 Network Configuration

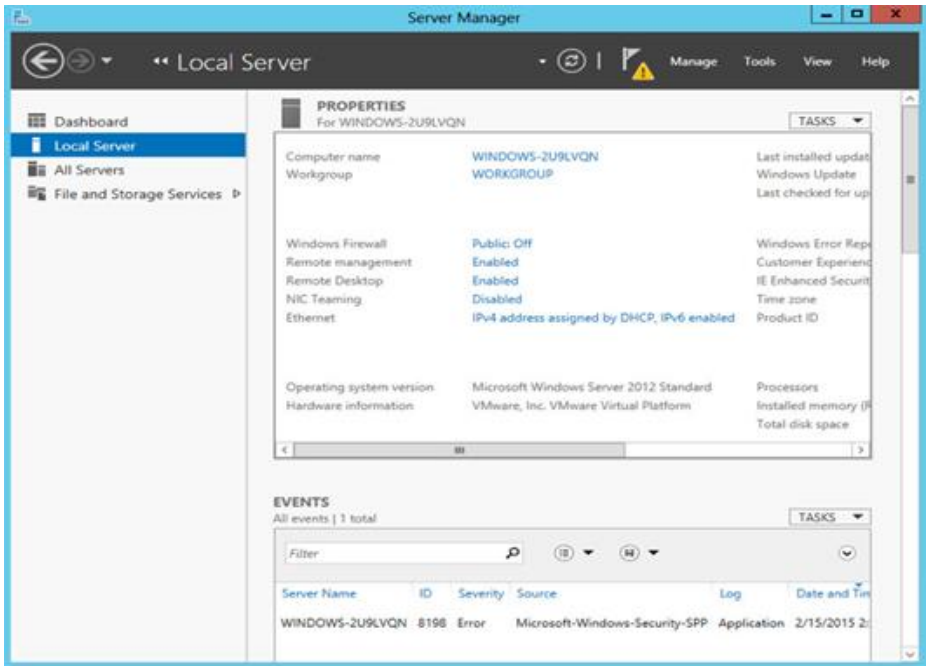
To successfully deploy GFC, you need to configure some basic settings such as IPv4 address, NetBIOS name, and domain membership through the **Windows Server 2016 or 2019 Server Manager** management console, which is automatically started after logging in to the GFC instance using the local **FASTAdmin** account.

Click “Local Server” in the left pane and click the blue text next to “Ethernet” to open the Network Connections available to this instance.

Virtual appliances typically provide a single Local Area Connection to guest operating systems, which is based on the 1Gbps **VMXNET3** interface.

© 2020 NetApp, Inc. All Rights Reserved.

Figure 6)



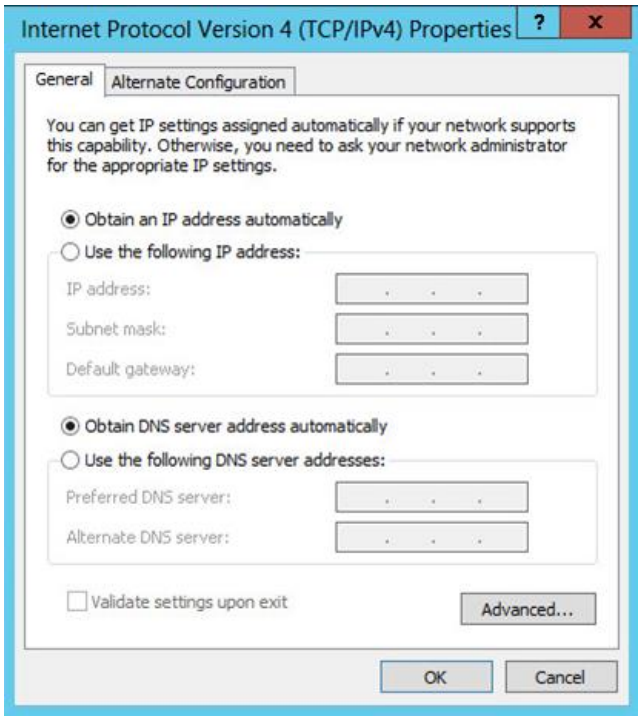
This document only covers the basic configuration of IPv4 addresses, subnet mask, gateway, and DNS server settings using the “Local Area Connection” virtual network adapter, which is applicable to any GFC appliance.

1. Right-click the “**Local Area Connection**” adapter
2. Click “**Properties**”
3. Select Internet Protocol 4 (TCP/IPv4)
4. Click “**Properties**”

This opens the basic IPv4 configuration window.

© 2020 NetApp, Inc. All Rights Reserved.

Figure 7)



In order to manually configure the IP address, gather network information from page 4 and fill out the following fields:

- IP Address
- Subnet mask
- Default Gateway
- Preferred DNS Server
- Alternate DNS Server
- Click "**OK**" to confirm configuration

The GFC instance is now configured to communicate with other devices on the network to join the Active Directory domain.

4.4 Active Directory Configuration

Please follow the NetBIOS and Domain configuration steps as outlined in this section.

Note: Screenshots used throughout this document based on Microsoft Windows Server 2012 R2. Your experience may vary from what is shown.

The GFC instance needs a unique NetBIOS computer name. It is recommended to adhere to the company's naming scheme for ease of management.

In many cases, the NetBIOS computer name represents a logical name including a geographical location, i.e.

- Core GFC instance located in Amsterdam

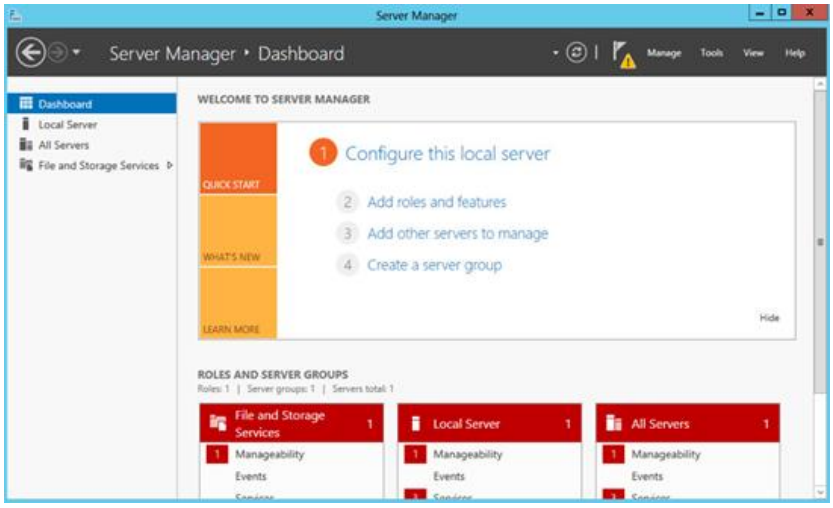
AMS-FAST1

- Edge GFC instance located in London

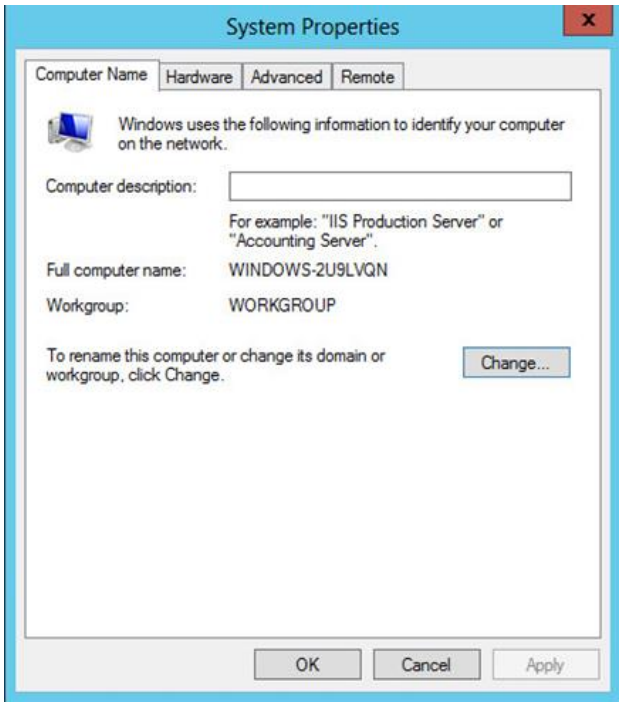
LON-FAST1

© 2020 NetApp, Inc. All Rights Reserved.

1. Use the Microsoft Windows Server 2016 and 2019 Server Manager console to configure the GFC instance's NetBIOS name by clicking "**Local Server**" in the left pane.



2. Click the blue entry next to "**Computer name**" to open the System Properties window.
3. Click the "**Change…**" button to open the Computer Name/Domain Changes window.



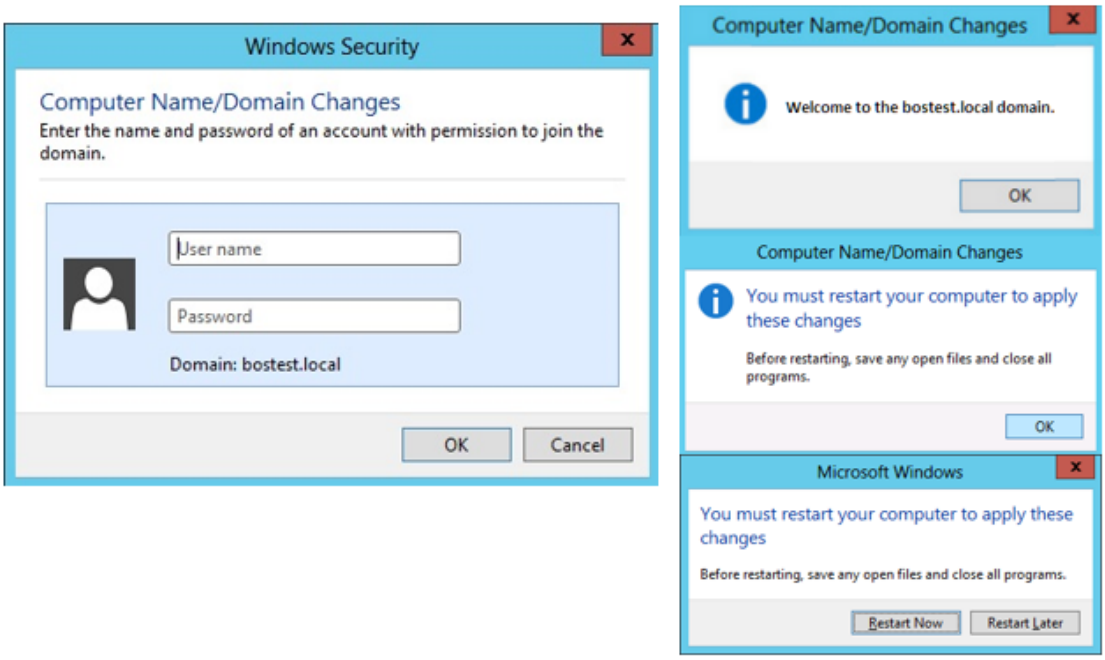
4. Type the desired NetBIOS name in the "**Computer Name**" field.
5. Select "**Member of**" Domain.
6. Type the Active Directory FQDN.
7. Confirm by clicking "**OK**".

Complete the Configuration:

1. Provide a Domain Administrator's **username** and **password**.

© 2020 NetApp, Inc. All Rights Reserved.

2. Confirm by clicking “**OK**”.



Once the GFC instance is successfully joined to your company’s Active Directory domain, perform a system reboot by clicking “**Restart Now**”.

4.5 Software Installation Package (Update)

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

Ensure that your GFC instances are up to date with the latest GA version available at http://www.talonstorage.com/support/downloads

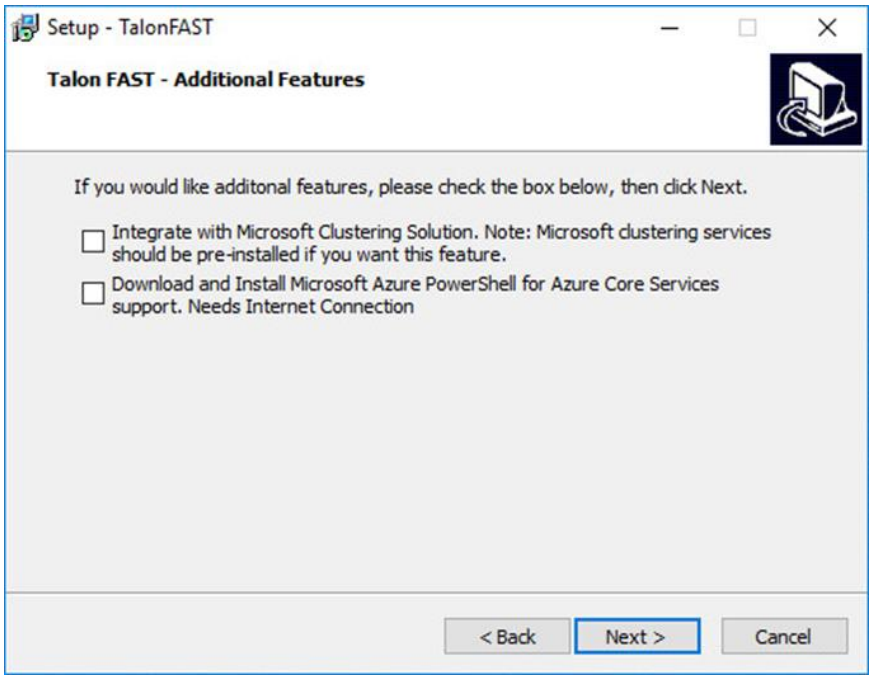
Note: This software package can also be used for pristine installations on Microsoft Windows Server 2016 Standard or Datacenter or Windows Server 2019 Standard or Datacenter edition or used as part of your upgrade strategy.

Below you can find the steps required to update the GFC installation package:

1. After saving the latest installation package to the desired Windows Server instance, double-click it to run the installation executable.

2. Click the "**Next**" Button to continue the process.
3. Optional: check the desired boxes when configuring the Core using Microsoft Clustering Services.

© 2020 NetApp, Inc. All Rights Reserved.



4. Click "**Next**" to continue.
5. Accept the Licensing Agreement and click “**Next**”.
6. Select the desired Installation Destination Location.

   Note: It is recommended that the default installation location be used.
7. Click “**Next**” to continue.
8. Select the Start Menu Folder.
9. Click “**Next**” to continue.
10. Verify the desired installation parameters and click “**Install**” to begin the installation.
11. The installation process will execute.
12. Once the installation has completed, reboot the server when prompted.

© 2020 NetApp, Inc. All Rights Reserved.

5 Licensing

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

Important: If you are using Cloud Manager to enable Global File Cache, you can skip this step. Cloud Manager automatically provisions the GFC Management Server instance alongside the GFC Core instance and enables entitlement / licensing.

See https://docs.netapp.com/us-en/occm/concept_gfc.html for a step-by-step walkthrough.

5.1 How It Works

When you deploy your first core instance in the datacenter or cloud, you can choose to designate that specific instance to become the LMS for your organization. This LMS instance is configured once, connects to the subscription service (HTTPS) and validates your subscription using the customer ID provided by our support/operations department upon enablement of the subscription.

Once you have deployed your LMS instance, you need to associate your edge instances with the LMS by providing your customer ID and the IP address of the LMS instance. This process can be executed manually or automated. For automation options, either through registry, GPO or PowerShell DSC, consult your GFC Solutions Engineer.

5.2 Subscription Updates

The subscription service is designed to simplify license management. Once you have renewed or extended your subscription, our support/operations department will centrally update the license details, i.e. the number of sites or subscription end date. Once LMS queries (HTTPS) the subscription service, the license details will be automatically updated on the LMS instance and the (new) license details will apply to your GFC core and edge instances.

5.3 Caching

The LMS instance gathers the subscription information, including the number of sites and the end date associated with the subscription. The LMS instance caches these details so, in case LMS is disconnected from the internet or the subscription service is unavailable, you can continue to deploy and validate your licenses.

5.4 Requirements

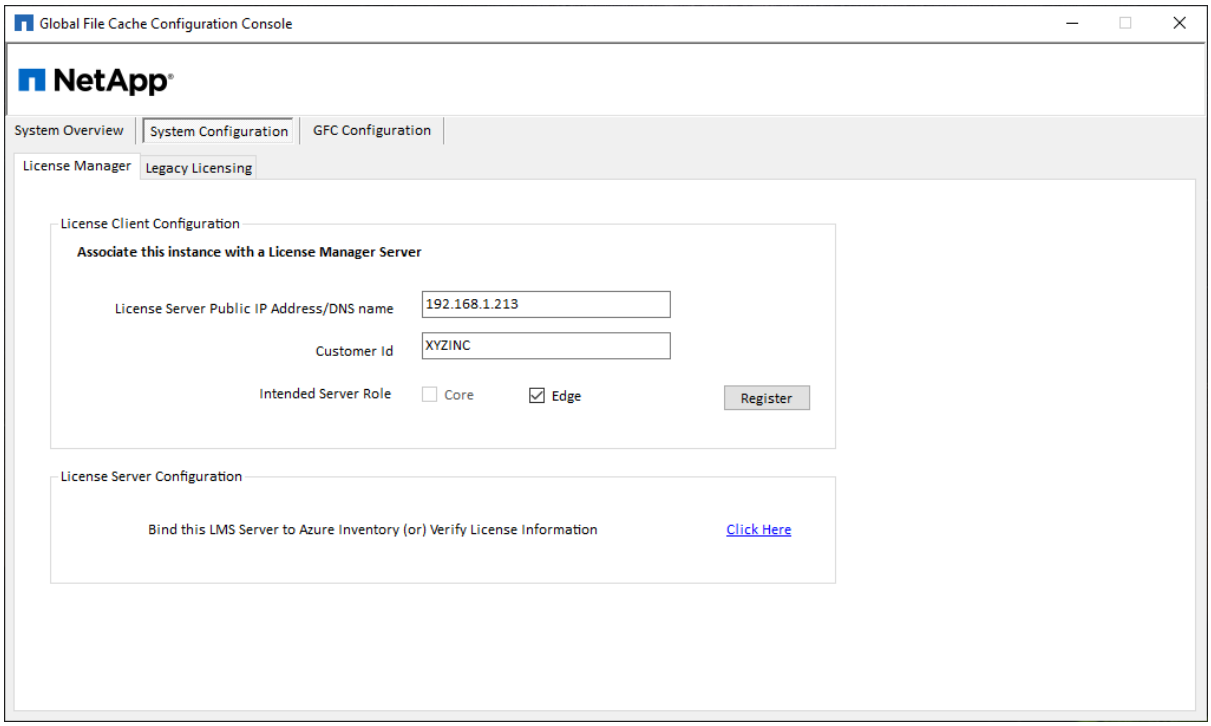
- The GFC LMS instance should be configured on a Microsoft Windows Server 2016 Standard or Datacenter edition or Windows Server 2019 Standard or Datacenter edition, preferably the GFC core instance in the datacenter or cloud.
- If you require a separate GFC LMS instance, you need to install the latest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

5.5 Deploying GFC LMS instance

In this example, we will configure the LMS service on an existing GFC core instance running GFC in the (on prem, hybrid or public cloud) datacenter. This is a one-time exercise that allows you to complete the GFC LMS deployment.

© 2020 NetApp, Inc. All Rights Reserved.

1. To start the LMS configuration, open the GFC Configuration Console from the designated GFC LMS instance (i.e. initial GFC core instance in the environment) and select the option in "**System Configuration**".



or open a web browser (Internet Explorer) and navigate to the following URL:

https://localhost/lms/api/v1/config/lmsconfig.html

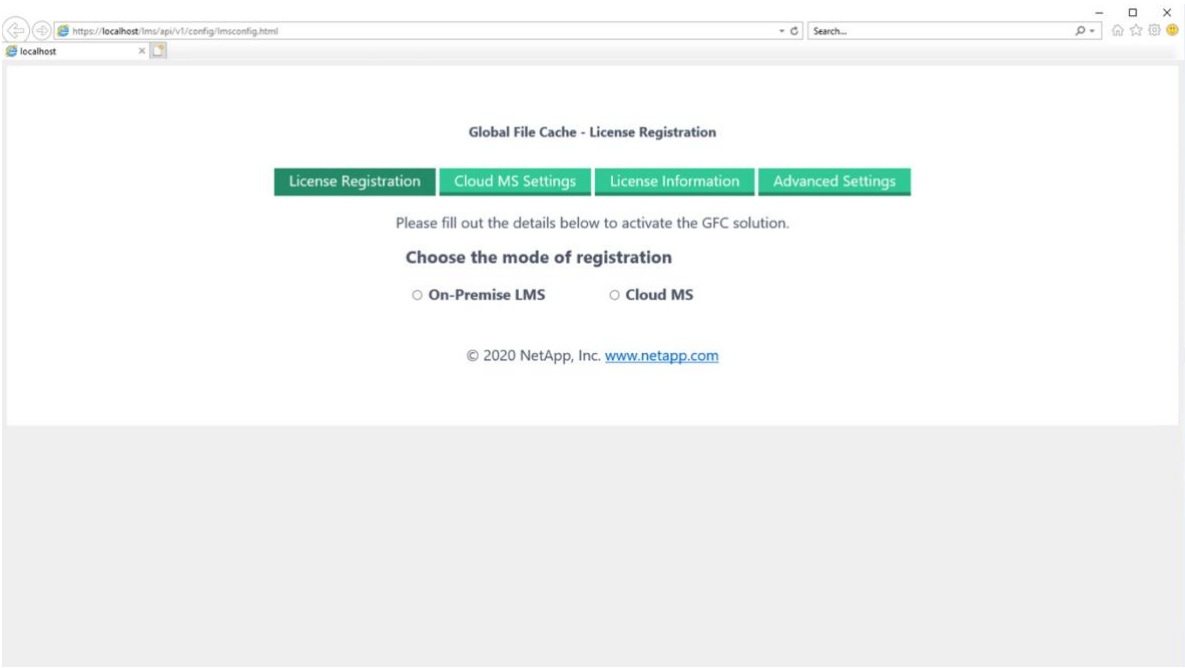
Note: you can also access the URL from a client workstation using the following URL using the IP address of the GFC Management Server or LMS server:

https://[ip address]/lms/api/v1/config/lmsconfig.html

2. Click "**Continue to this website (not recommended)**" to continue.

   A webpage will be presented, which allows you to configure the LMS or check existing license information.

© 2020 NetApp, Inc. All Rights Reserved.



3. Choose the mode of registration by selecting "**On-Premise LMS**" **or "Cloud MS"**.

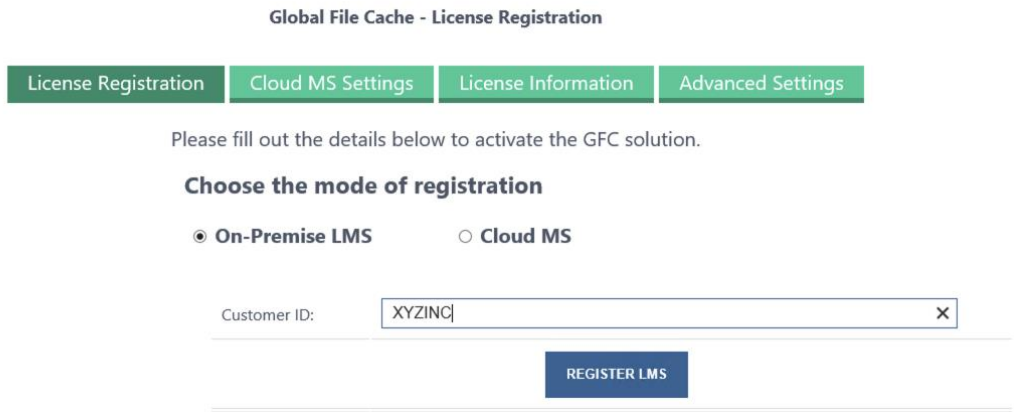
   "On-Premise LMS" is used for (existing) or trial customers that have received a Customer ID through NetApp Support.

   "Cloud MS" is used for customers that have purchased NetApp Global File Cache edge licenses from NetApp or its certified partners.

   Note: Your NSS credentials will be required to enable Global File Cache.

© 2020 NetApp, Inc. All Rights Reserved.

4. **“On Premise LMS”**

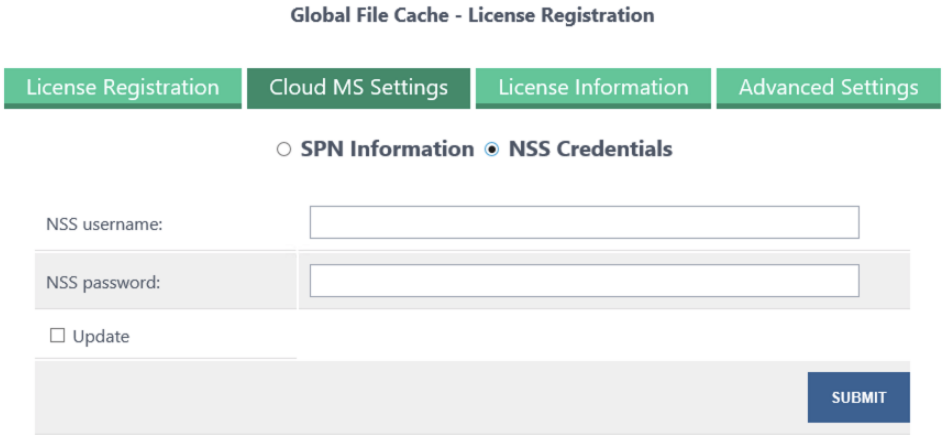


You will be prompted to enter the Customer ID (case sensitive) as provided by NetApp Support/operations department, i.e. XYZINC.

5. “Cloud MS”

In order to license and activate Global File Cache, you need to provide ONLY your NetApp NSS Credentials under the **“NSS Credentials”** section.

Click **“SUBMIT”** to complete the process.



© 2020 NetApp, Inc. All Rights Reserved.

6 Initial Configuration

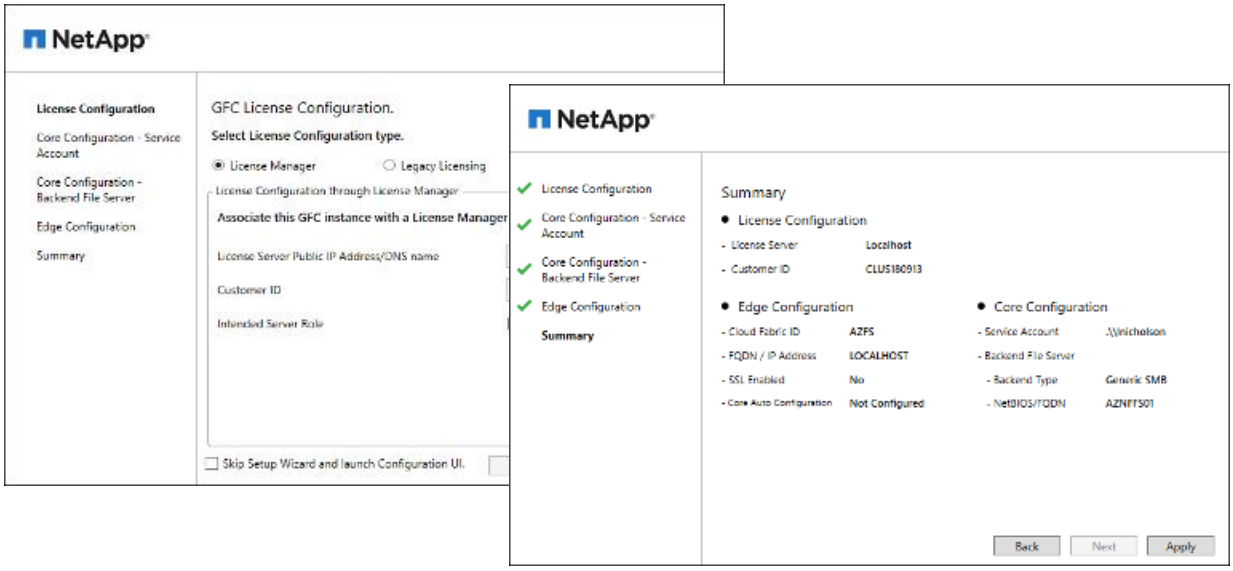
6.1 Initial Configuration Wizard

NetApp Global File Cache (GFC) includes a ‘Configuration Wizard’ for pristine installations of the software. This wizard will guide you through the process of associating your GFC instance with your existing license manager (see Section 5) and quickly deploy core or edge instances.

Note: This configuration wizard only applies to customers with a site-based subscription that have deployed a licensing server (see Section 5). If you do not have an LMS instance, follow the configuration steps as outlined in section 5.5 “Deploying GFC LMS instance” before starting the initial configuration wizard.

Once you completed the deployment of the GFC virtual instance and committed a reboot, you can start the configuration wizard by clicking the **Configuration Console** icon on the desktop.

Figure 8)



1. In the opening screen, select “**License Manager**” and click next. If you need to apply a legacy license (.XML file) select “**Legacy Licensing**,” you will be prompted to exit the wizard and use the Configuration Console to apply the license.
2. Follow the steps prompted to complete the licensing configuration using the IP address of your LMS instance and the customer ID provided by GFC.
3. Based on your selection GFC Edge or Core instance, you will be guided through the process of deploying basic settings associated with the configuration.

Note: You may skip the Configuration Wizard and launch the GFC Configuration UI by checking the box on the initial Configuration Wizard screen and clicking “Exit”.

© 2020 NetApp, Inc. All Rights Reserved.

6.2 Talon Configuration Console

Once the initial configuration wizard has completed or you've selected "**Legacy Licensing**" during the wizard, you can launch the **Configuration Console** from the desktop. The Configuration Console allows you to configure basic System Settings, GFC Core and Edge settings (See also Section 7):

GFC Core Instance

1. Provide the Service Account.

   Must be a member of backup operators group on the datacenter file server (i.e FS1).
2. Add the datacenter file server to the list of backend file servers i.e. FS1.
3. Configure Global / Server Exclusion Lists or Remote Inclusion Lists.
4. Configure Selectable File Handling.
5. Schedule Pre-population jobs.

GFC Edge Instance

1. License the Edge Instance (LMS or Legacy).
2. Associate the Edge instance with the Core instance at the datacenter or in the cloud.
   a. Cloud Fabric ID (Location)
   b. IP Address / FQDN of the GFC Core instance
3. Schedule Edge Pre-population jobs
4. Advanced Settings

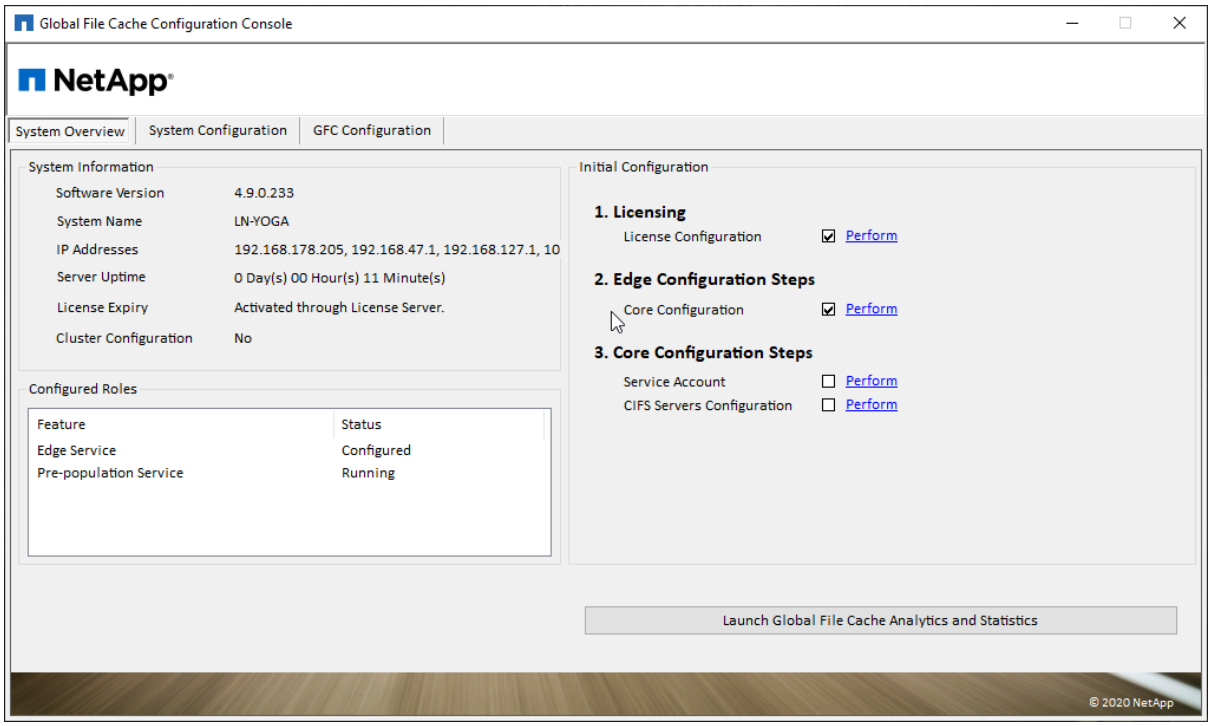
Registering your GFC Core or Edge instance with GFC LMS (Optional)

Note: The following steps are only required if you skipped the initial configuration wizard or upgraded from a previous release.

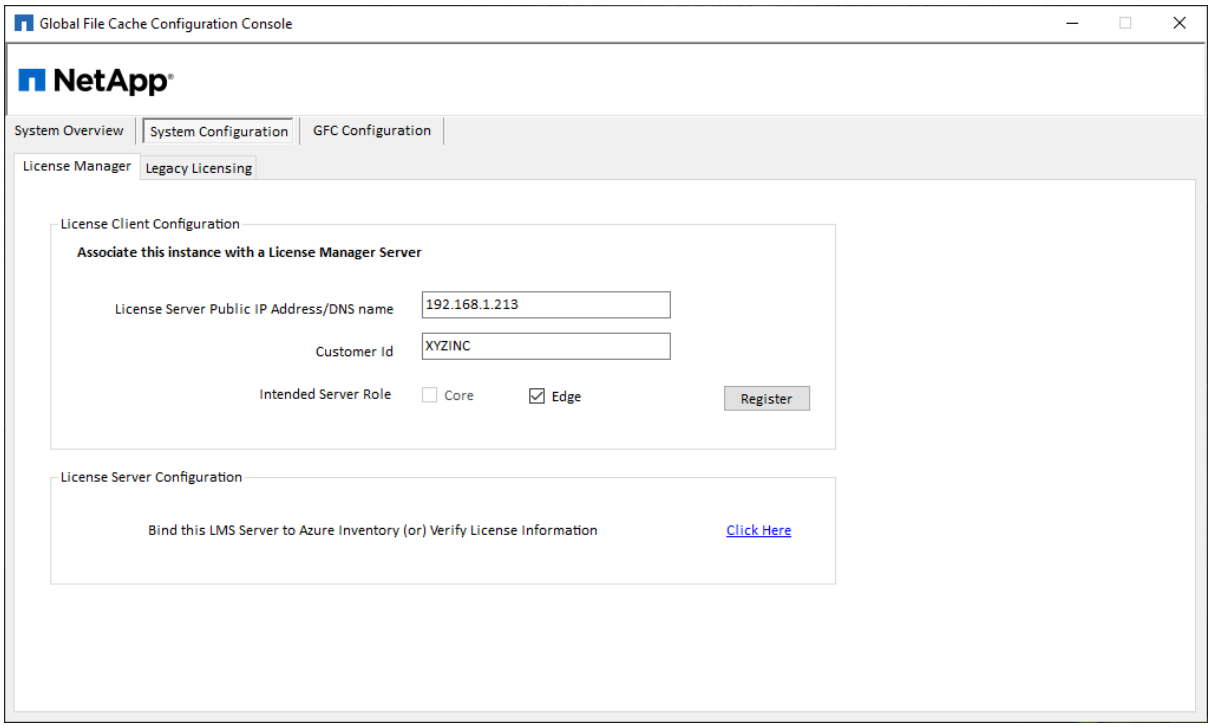
Now that the GFC LMS is correctly registered and associated with the subscription service, you need to license the first host in the environment, which is typically the Core instance.

1. Open the **Configuration Console** from the desktop.

© 2020 NetApp, Inc. All Rights Reserved.



2. Click on “**Perform**” next to License Configuration in the Initial Configuration section or navigate to the “**System Configuration**” tab, which opens the License Manager tab.

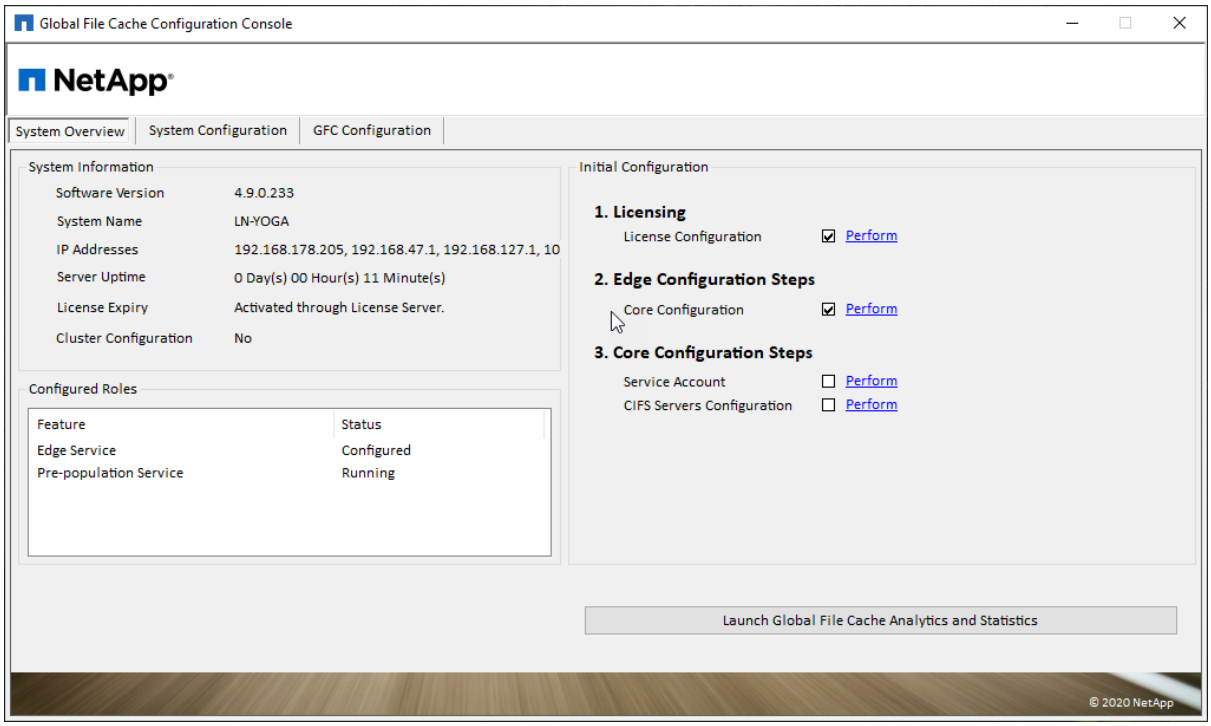


3. Provide the IP address of the GFC LMS instance, i.e. 1.2.3.4 and Customer ID (i.e. XYZINC)
4. Select the intended server role, Core or Edge and click “**Register**” to confirm.

© 2020 NetApp, Inc. All Rights Reserved.

Once this GFC instance has been configured it will register with the GFC LMS instance and a confirmation message is shown that the site has been registered successfully.

5. Click "**OK**" to close this message.



6. Once completed you can check that the licensing has been completed by navigating back to the "**System Overview**" tab of the GFC Configuration Console. License Expiry will display "**Never (Activated through License Server)**".
7. Repeat this process "**Registering your GFC** Core or Edge instance with **GFC LMS**" for each GFC instance in your environment.

Note: The configuration of the GFC core or edge instances can be automated through either GPO or PowerShell Desired-State Configuration. Consult your GFC Solutions Engineer or NetApp Support to discuss the options.

© 2020 NetApp, Inc. All Rights Reserved.

7 Designing and Deploying NetApp Global File Cache Core

Depending on your requirements you may need to deploy one or multiple NetApp Global File Cache (GFC) core instances to create the GFC Fabric. The core instance is designed to act as a 'traffic cop' between your distributed GFC edge instances and the datacenter file server resources, i.e. file shares, folders and files.

The GFC core instance creates the GFC Fabric which allows customers to centralize and consolidate unstructured data into a 'single set of data,' whether it resides on one or multiple storage platforms in the on prem, hybrid or public cloud.

When you are designing your GFC deployment you need to determine what's right for your environment in terms of scale, availability of resources and in terms of redundancy.

GFC core can be deployed in the following ways:

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

Note: It is recommended to deploy GFC core instance as a virtual machine on a hypervisor platform that leverages high availability options.

7.1 GFC Core Stand-Alone Instance

When deploying a GFC core stand-alone instance, you need to provision a single virtual machine, either by deploying Windows Server 2016 Standard or Datacenter Edition or Windows Server 2016 Standard or Datacenter Edition or using the GFC.OVA or .VHD template which includes the three Windows Server operating system of choice and GFC.

Quick steps:

1. Deploy GFC Virtual Template or Windows Server 2016 virtual machine or Windows Server 2019 Standard or Datacenter edition
2. Ensure virtual machine is connected to the network, joined to the domain and accessible through RDP
3. Install the latest GFC Software Installation Package (Update)
4. License the GFC instance through the License Manager Server (see Section 5)
5. Configure the GFC Core role.

7.2 GFC Core Load Distributed Design

Enterprise customers that require multiple GFC core instances to ensure optimal scalability for their environment can leverage a distributed model of multiple core instances, including a cold-standby for disaster recovery. This model can also be leveraged to design a multi-fabric deployment with multiple active/active datacenters or to failover to a DR site, either in a separate location or in the cloud.

The model below allows you to provision multiple (i.e. region-specific) core instances, distribute the load between edges in a specific region to access the central data sets provided by the GFC Fabric.

In case a GFC core instance fails, and can't recovered in time, you can 'replace' the failed GFC core instance with a 'cold' standby instance by either changing the IP address of the 'cold' standby instance or updating the DNS record associated with the edge-to-core association (i.e. IP address, Cloud Fabric ID configured on the edge).

Note: Consult your GFC Solutions Engineer to discuss the best options for your enterprise deployment

© 2020 NetApp, Inc. All Rights Reserved.

7.3 Configuring GFC Core instance – Service Account

Once you have identified the right deployment strategy for your organization, provisioned the required VM instances, and have completed the licensing part (LMS), you need to start the core configuration.

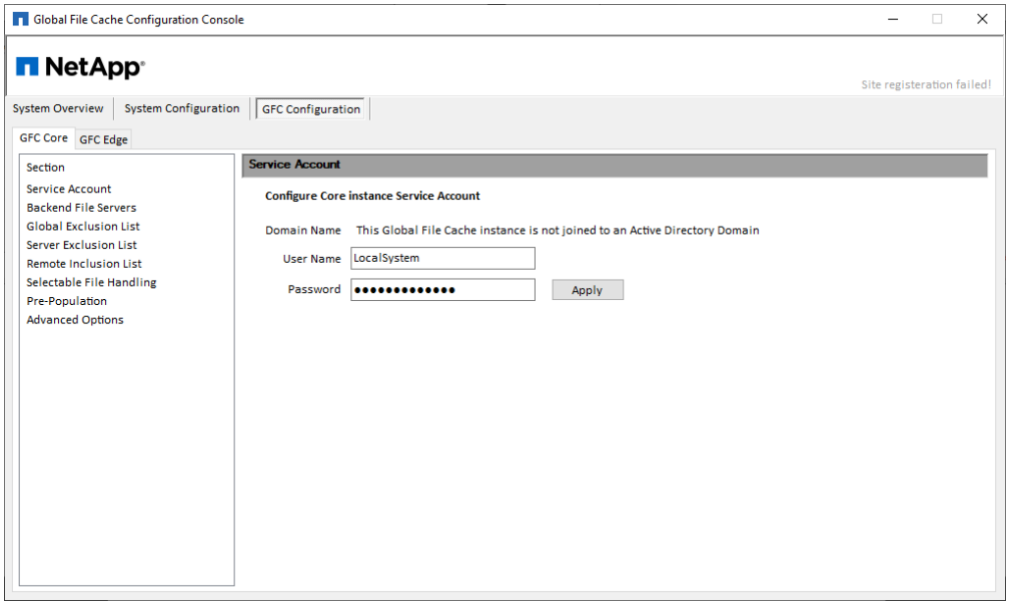
When a GFC instance is designated the Core role, GFC Edge instances will connect to it to access datacenter fileserver resources. The services on this instance run as a specific domain user account. This account, also known as the “Service Account”, must have the following privileges on each of the SMB servers that will be associated with the GFC Core instance:

1. The provisioned Service Account must be a domain user.

   Depending on the level of restrictions and GPOs in the network environment, this account may require domain admin privileges.
2. It must have “**Run as a Service**” privileges.
3. The password should be set to “**Never Expire**”.
4. The account option “**User must change password at next logon**” should be **DISABLED** (unchecked).
5. Must be a member of the backend fileserver local **Backup Operators** groups.
6. Any shares that will be exposed through GFC must allow the “**Everyone**” group “**Full Control**” at the share level, while restricting permissions through NTFS permissions.

To configure the Service Account **on your core:**

1. Click the tab “**System Overview**” and click “**Perform**” next to the unchecked “**Service Account**” step listed in the “3. Core Configuration Steps” section of the Initial Configuration assistant.
2. This opens a new tab, “**GFC Core**” and shows the section “Service Account**”**. Enter the **User Name** and **Password** of the Service Account created in Active Directory.
3. Click “**Apply**” and confirm the configuration of the Service Account.



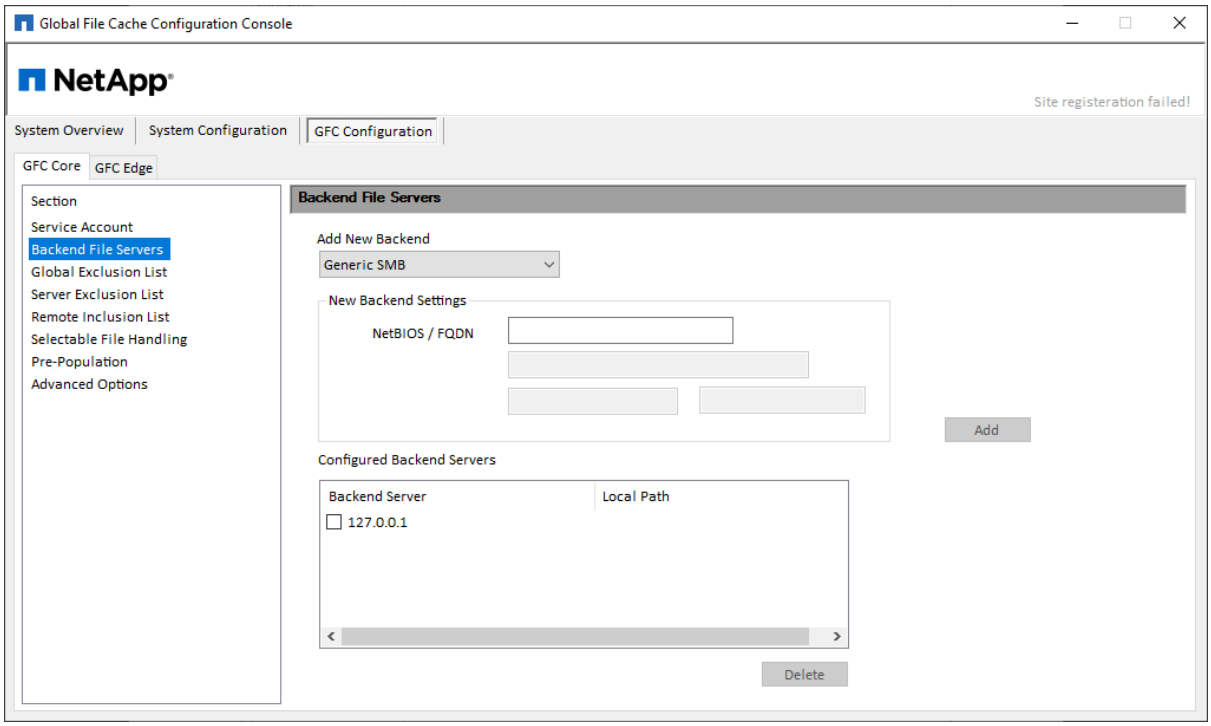
7.4 Configuring GFC Core instance – Backend File Servers

GFC core instances extend central file shares from configured datacenter backend file servers. GFC can also be configured in multiple ways to present a local share or an iSCSI LUN.

Please follow the steps below to connect file servers to the GFC Core instance.

© 2020 NetApp, Inc. All Rights Reserved.

1. Click the “**Backend File Servers**” item in the “**GFC Core**” tab of the Configuration Console or use the “**Backend File Servers Configuration**” step listed in the “3. Core Configuration Steps” section of the Initial Configuration assistant.
2. Select “**Generic SMB**,” “**DAS/iSCSI Mount**,” or “**Azure Files Storage**” depending on the backend file server to be added.



3. To add a generic SMB server, provide a NetBIOS name or FQDN in the “**Add New Backend**” field containing the backend file server to publish throughout all connected GFC Edge servers.
4. Click the “**Add**” button to add the server to the “**Configured Backend Servers**” list. The changes are applied directly to the GFC Core server configuration without displaying a confirmation box.
5. To add data from a local path or resource, select “**DAS/iSCSI Mount**” from the dropdown and enter the Storage Name of the resource name as you wish it to display. Enter the path of the resource (Ex. F:\Data) containing shares and click “**Add**.” The changes are applied directly to the GFC Core server configuration without displaying a confirmation box.

   For DAS/iSCSI configuration, a storage volume and NTFS filesystem must have already been created on the local GFC core instance prior to this configuration.
6. To add a Microsoft Azure Files storage share, select “**Azure Files Storage**” from the dropdown menu and check the box labeled “**Enable GFC Azure Files Mode**.” Enter the FQDN of the Storage Account for Azure Files. Enter the information in the associated Azure Credentials fields:
   c. Left Field — Enter the associated Azure Storage Account Name.
   d. Right field — Enter the associated Azure Storage Account Primary Key.
7. Click “**Add**” to add the Azure Files Storage Account to the Configured Backend Servers list.

Note: You must allow the “**Everyone**” user group “**Full Control**” permissions on the ACL of each share on the backend file server.

Note: Using a DFS root or alias as your backend file server is not recommended and can lead to data loss.

© 2020 NetApp, Inc. All Rights Reserved.

7.5 GFC Core Advanced Features

Note: The following advanced Core features must be configured identically on each Core server if utilizing Microsoft Cluster Services.

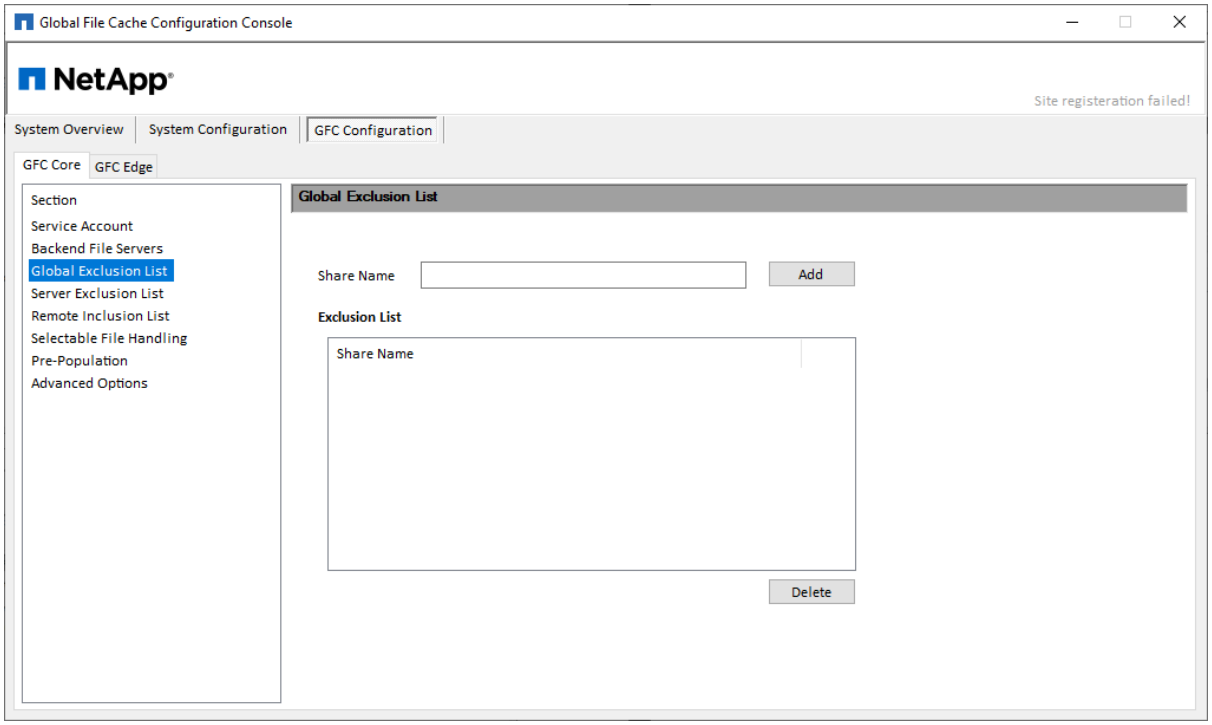
7.6 Global Exclusion List

The Global Exclusion List feature allows SMB/CIFS file server shares to be hidden from all GFC Edge servers, and subsequently from branch office end user clients. The shares with the configured names will not be available through GFC from any datacenter file server configured to the GFC Core server.

This feature may be used when there are multiple file shares with the same name on several backend file servers.

1. To hide named shares from all Edge instances.
2. Open the **Configuration Console**.
3. Select the "**Configuration**" tab and ensure that the "**GFC Core**" tab is active.
4. Click "**Global Exclusion List**".
5. Enter a "**Share Name**" to prevent distribution through GFC.
6. Click "**Add**" to add a share name to the exclusion list.

   Once added to the list, the change is applied.



7.7 Server Exclusion List

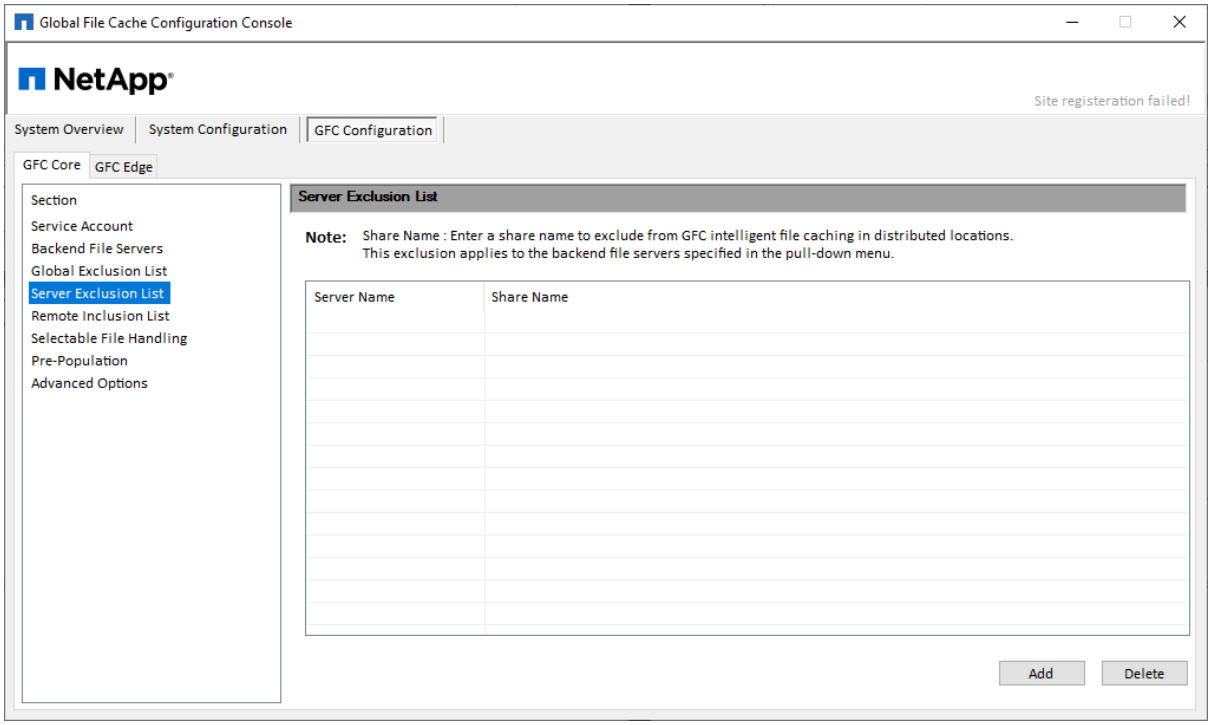
The Server Exclusion List feature prevents specified shares from individual SMB/CIFS file servers from being shared with Edge servers via GFC. This feature can be used to achieve a level of granularity in control of what shares are presented as available via GFC to end users.

To hide specific shares from all Edge instances

1. Open the **Configuration Console**.
2. Select the "**Configuration**" tab, and select the "**GFC Core**" tab.

© 2020 NetApp, Inc. All Rights Reserved.

3. Click “**Server Exclusion List**”.
4. Click the “**Add**” button to display the “**Add Server Exclusion List**” window.
5. Select the desired backend file server from the dropdown menu.
6. Enter a “**Share Name**” to prevent distribution through GFC.
7. Click “**Apply**” to add a share name to the exclusion list.
   Once added to the list, the change is applied.
8. Repeat this process for each server and share combination you wish to exclude.



7.8 Remote Inclusion List

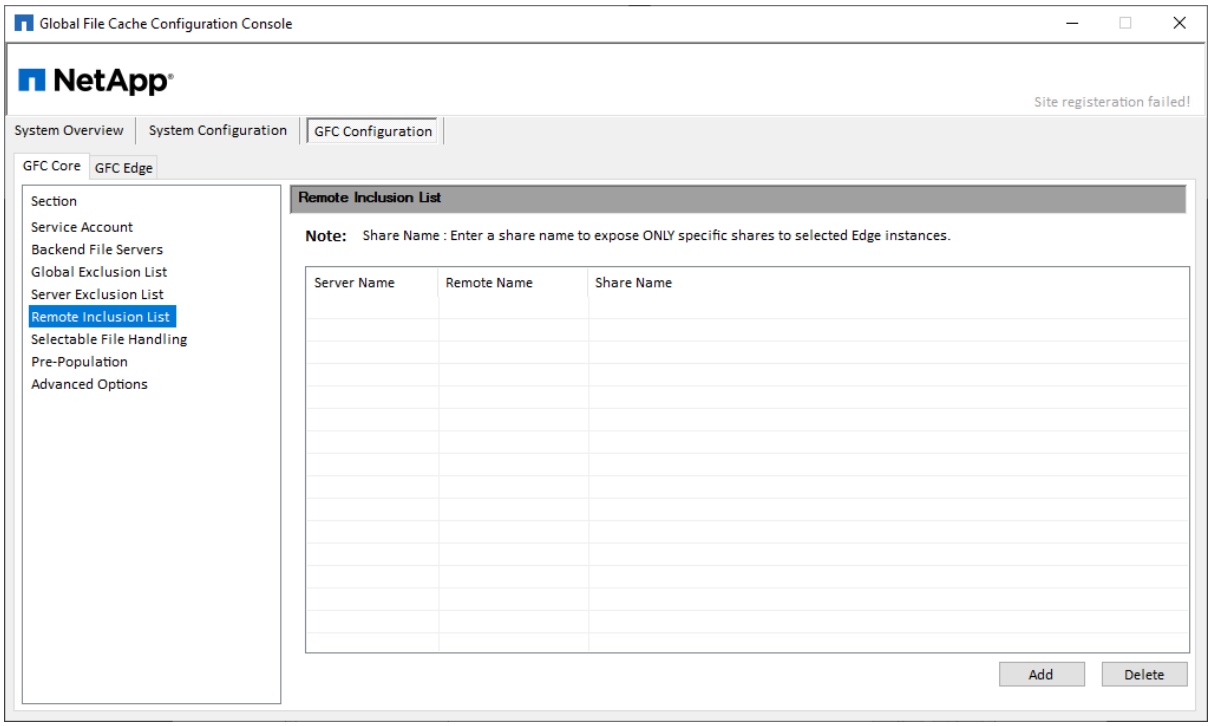
The Remote Inclusion List feature in GFC provides a method of control to expose specific shares to specified Edge servers. These may be used in the case where a branch office needs access to a share that has previously been excluded or a specific named share.

To allow inclusion of specific shares to specific Edge instances

1. Open the Configuration Console.
2. Select the “**Configuration**” tab, and select the “**GFC Core**” tab.
3. Click “**Remote Inclusion List**”.
4. Click the “**Add**” button to display the “**Add Remote Inclusion List**” window.
5. Select the desired backend CIFS file server from the dropdown menu.
6. Select a target Edge server “**Remote Name**” from the second dropdown menu.
7. Enter a “**Share name to include**” that exists on the datacenter file server in the dropdown menu.
8. Click “**Apply**” to add a share name to the inclusion list.
   Once added to the list, the change is applied.
9. Repeat this process for each server and share combination you wish to include.

© 2020 NetApp, Inc. All Rights Reserved.

Figure 9)



7.9 Selectable File Handling

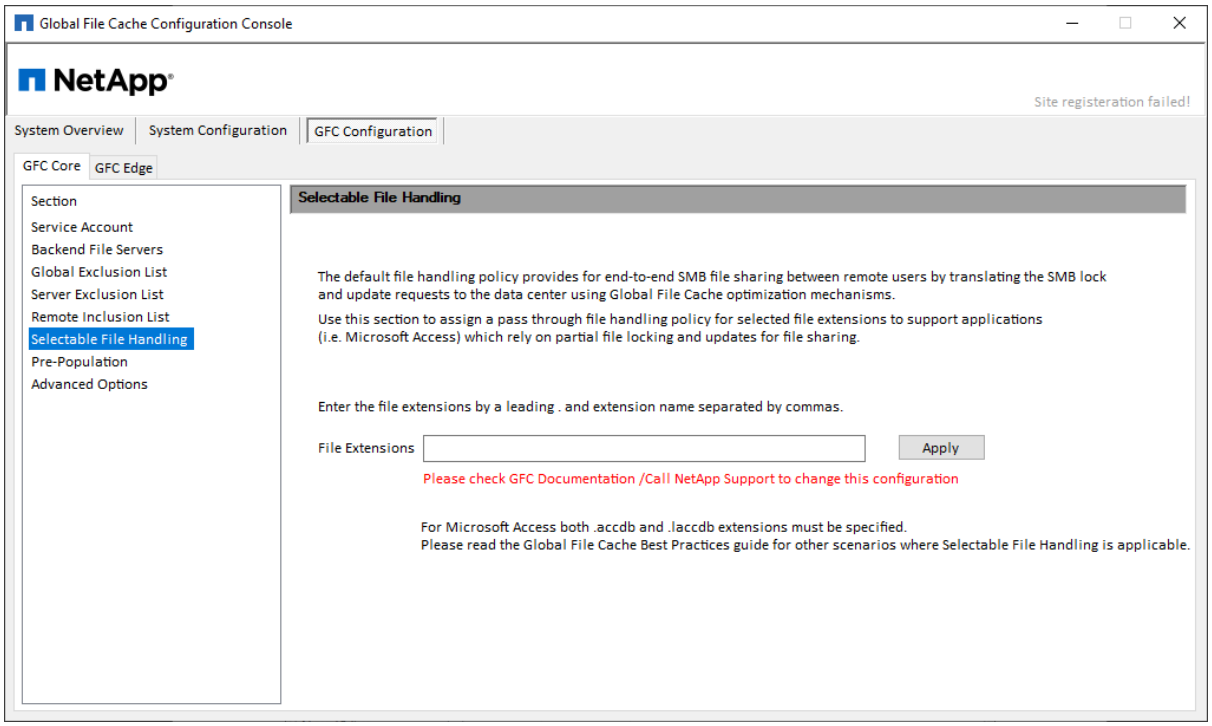
Certain applications, such as Microsoft Access or Autodesk Revit, rely on partial file locking and partial file updates for file sharing coherency. In order to use these kinds of applications with GFC, you must first disable file locking for the file extensions associated with the application. Pass-through policies are applied to file patterns globally and cannot differ between Edge servers attached to the configured Core.

To modify Selectable File Handling

1. Open the **Configuration Console**.
2. Select the "**Configuration**" tab, followed by selecting the "**GFC Core**" tab.
3. Click "**Selectable File Handling**".
4. Enter the file type extensions (used by the application) separated by commas and preceded by a period in the "**File Extensions**" text box.
5. Click "**Apply**" to apply the settings, a confirmation box will appear.
6. Click "**Yes**" to apply the changes immediately.

© 2020 NetApp, Inc. All Rights Reserved.

Figure 10)



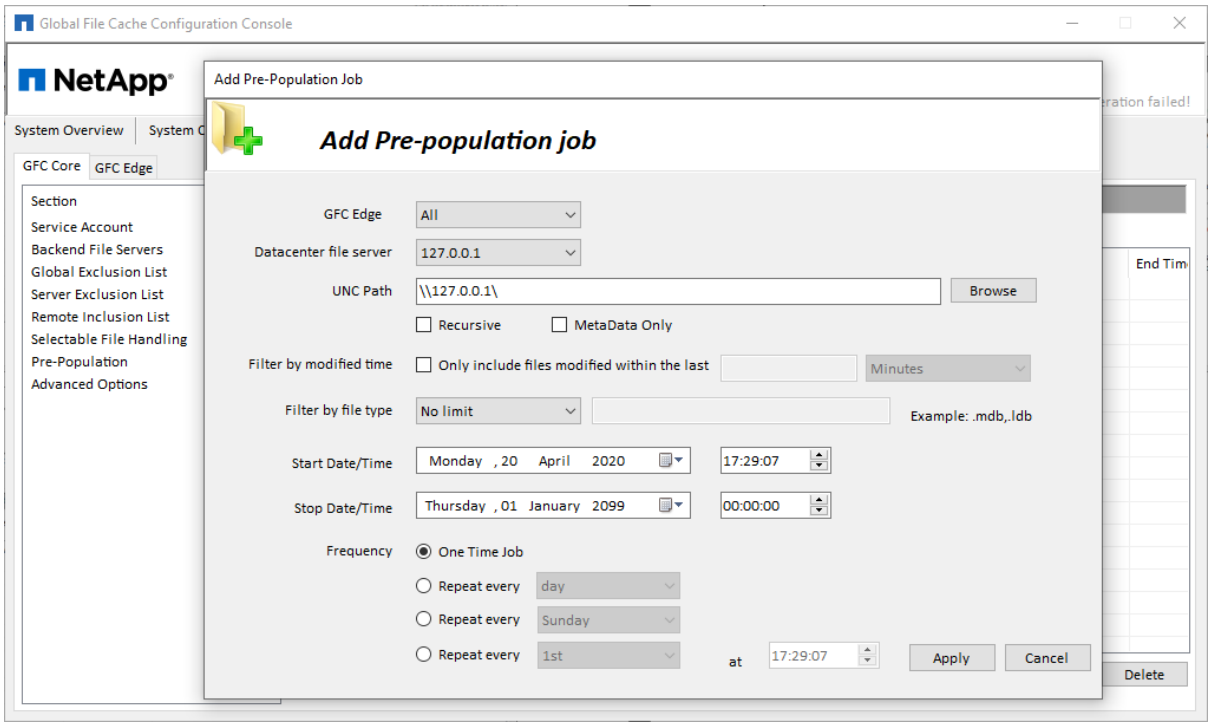
7.10 Core Pre-population

The pre-population feature updates shares, directories, folders, and/or files from datacenter servers to the branch office Edge server(s) at predetermined times and frequencies. This pre-populates GFC Edge caches with data that will be used by their connected clients, creating a ‘warm’ cache on the Edge server. Branch office clients access files from the warm cache much faster than ‘cold’ files, those that need to be fetched from datacenter servers and then sent over the WAN.

Pre-population jobs can be scheduled from the Core or Edge instance, which triggers data fetches from the associated GFC Edge server(s). All times associated with pre-population correspond to the Edge server’s local time.

© 2020 NetApp, Inc. All Rights Reserved.

Figure 11)



Note: Before you define, schedule, or edit a pre-population job, the GFC core instance requires at least one associated datacenter file server as configured in the "**Backend File Servers**" section of the UI.

The Pre-Population page displays a list of data push jobs scheduled from the Core to the GFC Edge servers. The Pre-population window displays the following information for each scheduled pre-population job.

Table 1)

Field name	Description
JobID	An automatically generated job identification number
Edge	Name of the GFC Edge server to be pre-populated with data (or All if data will be pushed from the specified server to all Edge servers).
Server	Name of the data center file server
Path	Path of the folder on the data center server with information to be shared, for example, \\myserver\folder\sharefolder
Recursive	If checked, the pre-population data is recursive, and will transfer the files in the indicated directory as well as all its subdirectories. If No, only the specified folder will be pre-populated.
Metadata Only	If checked, the pre-population mechanism only populates metadata from the specified files and directories, this does not write data to the branch office Edge cache.
File Modified Time	File modification times, if only data with specific modified by dates are to be pre-populated

© 2020 NetApp, Inc. All Rights Reserved.

File Extension	File extensions of any file types to be specifically included in or excluded from the Pre-population job
Start Time	Start time of the pre-population job (Edge server local time)
End Time	End time of the pre-population job if a one-time job (Edge server local time)
Frequency	Displays 'One Time' if a single job or displays the frequency of a recurring job
Stop Time	End time of the pre-population job schedule if a recurring job (Edge Server local time)

To Configure and Schedule a Pre-Population Job

1. Open the **Configuration Console**.
2. Select the "**Configuration**" tab and then select the "**GFC Core**" tab.
3. Click "**Pre-Population**".
4. Click "**Add**" from the Pre-population page. The "**Add Pre-Population Job**" window opens.
   a. Click the "**Edge**" drop-down menu and select a GFC Edge server to receive the files, or choose "**All**" to pre-populate files to all of the GFC Edges connected to the GFC Core.
   b. From the "**Datacenter File Server**" drop-down menu, select the file server with the data to be pre-populated.
   c. In the "**UNC Path**" field, enter the UNC path for the file or directory to be pre-populated (for example, `\\<server_name>\<share_name>\<directory>`).
   d. **(Optional)** Enable the "**Recursive**" checkbox to make the pre-population job recursive, which transfers the files in the indicated directory as well as all its subdirectories. Pre-population jobs that are not recursive only transfer the files in the directory indicated by the path; they do not transfer files within any subdirectories.
   e. **(Optional)** Enable the "**Metadata Only**" checkbox to only prepopulate Edge instances with specified Metadata. If this is unchecked, specified directories and files will be written to the Edge's local file cache.
   f. **(Optional)** Enable the "**Filter by Modified Time**" checkbox to pre-populate only those files modified within a specified time interval. Click the drop-down menu to specify a time frame (minutes, hours, days) then type the number of minutes, hours, or days in the box.
   g. **(Optional)** To pre-populate only specific types of data, click the dropdown box next to "**Filter by file type**" and select "**No Limit**," "**Include**," or "**Exclude**." Type the file extensions (case sensitive) of the files to include or exclude in the entry blank, for example, .docx, .pdf, .html, or .xlsx. File extensions should be preceded by a period and multiple extensions must be separated by commas.
   h. In the "**Start Date/Time**" and "**End Date/Time**" fields, set the start and end dates and times for the initial and final data subject to pre-population. If this is a one-time job, the "**Start Time**" field needs to be populated at least 20 minutes in advance and the "**End Time**" field should be set 24 hours later.
   i. **(Optional)** Select the desired "**Repeat every…**" radio button if the push should repeat multiple times. For repeating jobs, the "**Start Date/Time**" specifies the beginning of the window for which a repeating job can occur. A repeating job will begin on the time and days specified in the "**Frequency**" column, as long as those days are within the "**Start Date/Time**" and "**End Date/Time**" window.

      Set the end date and time for a repeating job using the drop-down menus next to the "**End Time**" field.

© 2020 NetApp, Inc. All Rights Reserved.

Select a “**Frequency**” radio button to select the frequency the push job will repeat.

j. To repeat by day interval: Click the “**Repeat every <day>**” radio button. By default, the repetitive push job is scheduled to repeat every day at the specified time. To repeat the job on other dates, click the drop-down list and select one of a series of dates ranging from every day to every 10 days or every fifteenth day. Next, enter the desired hour, minute, and second to specify a time that the pre-population job should occur.

k. To repeat by day of the week: Click the “**Repeat every <day of the week>**” radio button and click the drop-down list to select the day of the week the pre-population job could occur. Next, enter the desired hour, minute, and second to specify a time that the pre-population job should occur on the specified day.

l. To repeat by date of the month: Click the “**Repeat every <day of the month>**” radio button, then click the drop-down list to select the numerical date of the month that the pre-population job should occur. Next, enter the desired hour, minute, and second to specify a time that the pre-population job should occur.

Note: Jobs scheduled for the fifteenth and thirtieth of the month will only occur once in February, on the 15th. Since it only has 28 or 29 days, the job will not repeat again until the next scheduled date on the 15th of March. Other months that have only 30 days will not complete the Pre-population job if it is specified to execute on the 31st.

5. Click “**Apply**” to commit the pre-population job.
6. The “**Add Pre-Population Job**” window will close, and the new job will display in the table on the Pre-population page.
7. To configure a second scheduled pre-population job, repeat the process.
8. To edit a Pre-population job, click to highlight the job you wish to change and click the “**Edit**” button to change parameters.
9. Jobs can be deleted by highlighting the desired job and clicking the “**Delete**” button and confirming the action.

Note:

When scheduling pre-population jobs, all job times are relative to the time zone of the GFC Edge instance

Pre-population jobs should be scheduled at least 20 minutes ahead of the current time in the Edge’s local time zone to allow Edges to pick up the newly scheduled jobs

Pre-population jobs should be scheduled to run during non-business hours. Running pre-population jobs during business hours will impact user performance

Pre-population can be listed, added and deleted using the GFC PowerShell scripts. See Appendix C for more details and examples

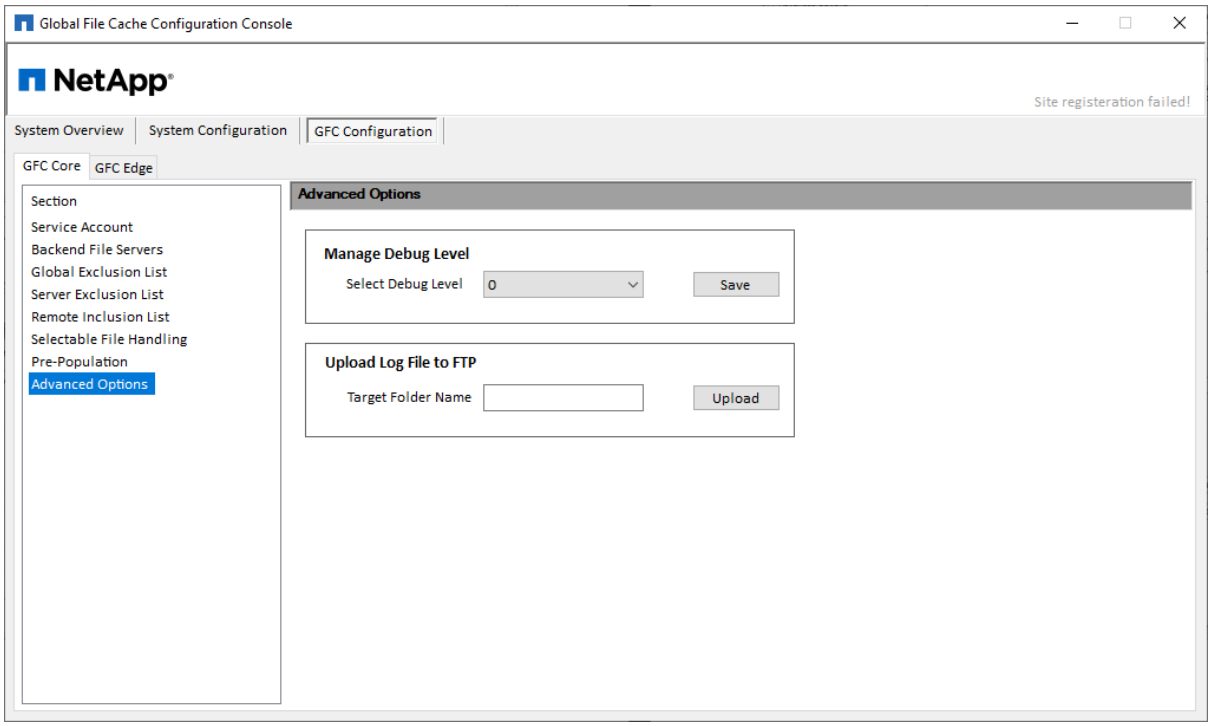
7.11 Core Advanced Options

Advanced Options give IT Administrators the ability to set the desired Debug Level for additional NetApp Support or Engineering information or troubleshooting. Additionally, a customer-specific folder can be automatically created and relevant debug logs automatically uploaded using the associated Advanced Options.

Note: These should only be modified or utilized as instructed by a member of NetApp Support. Please contact NetApp Support for any questions or prior to sending any log files.

© 2020 NetApp, Inc. All Rights Reserved.

Figure 12)



Manage Debug Level

This feature allows for more verbose (higher numbers, MAX: 9) debug logging.

Upload Log File to FTP

This feature enables a direct transfer of requested log files to NetApp Support.

© 2020 NetApp, Inc. All Rights Reserved.

8 Designing and Deploying NetApp Global File Cache Edge

Depending on your requirements you may need to deploy one or multiple NetApp Global File Cache (GFC) 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 GFC core instance. The GFC edge should contain a “D:\” NTFS Volume which contains the cached files within the branch office.

For the GFC edge it is important to understand the sizing guideline in Section 3.4 of the User Guide. This will assist in making the correct design for your GFC 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.

GFC edge can be deployed in the following ways:

- GFC edge stand-alone instance.
- GFC edge multi-edge deployment.

8.1 GFC stand-alone instance

When deploying a GFC edge stand-alone instance, you need to provision a single virtual machine, either by deploying Windows Server 2016 Standard or Datacenter Edition or Windows Server 2019 Standard or Datacenter Edition or using the GFC.OVA or .VHD template which includes the three Windows Server operating system of choice and GFC.

Quick steps

1. Deploy GFC Virtual Template or Windows Server 2016 virtual machine or Windows Server 2019 Standard or Datacenter edition.
2. Ensure virtual machine is connected to the network, joined to the domain and accessible through RDP.
3. Install the latest GFC.
4. License the GFC instance through the License Manager Server (see Section 5).
5. Configure the GFC Edge role.

8.2 GFC Edge Multi-Edge Deployment

For sites that have more users than the sizing guidelines dictate ‘concurrent sessions’ AND the datasets are used by all of the users, meaning we can’t separate the data to be associated with specific groups of users (i.e. Share1 is only used by Group HR which is only **X** users, and Share2 is only used by Group Finance which is Y users), we recommend to extend the user’s sessions to a secondary (or 3rd) edge using a local Stand-alone DFS namespace in the respective site.

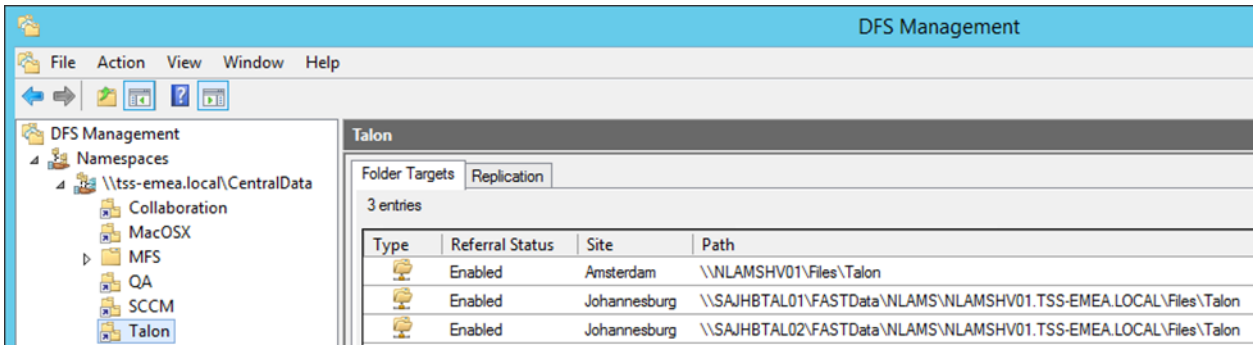
This means each GFC Edge instance is configured as a ‘stand-alone’ server instance in that site, with a unique NetBIOS name and IP address for each Edge instance and a dedicated cache volume for each separate Edge instance, which subsequently presents the local FASTData virtual file share(s) as part of a local stand-alone DFS root, which includes all of the feasible targets in that site as a valid target.

Each edge instance presents the central data hosted on the backend file server platform through a unique UNC path:

- `Edge1: \\Edge1\FASTData\Talon\FS1\Share\Folder\`
- `Edge2: \\Edge2\FASTData\Talon\FS1\Share\Folder\`
- `Edge3: \\Edge3\FASTData\Talon\FS1\Share\Folder\`

© 2020 NetApp, Inc. All Rights Reserved.

Figure 13)



In order to facilitate for load balancing, a local stand-alone DFS namespace needs to be configured on each GFC edge instance, meaning that each edge hosts a DFS root that contains a DFS link with the primary target (the local FASTData share or subfolder on that Edge) and secondary targets (corresponding FASTData share or folder on other edges in that site).

This model allows it to actively distribute the load between stand-alone DFS-N targets, which means that User1 will use Edge1 and User2 will use Edge2, etc. This selection is based on the round-robin principle, which means that User1 could use Edge2 any other time of day as the cache timer expires for the namespace and associated targets. In that case it could be that a file that was previously warm (on Edge1) is now cold (on Edge2). If you schedule a nightly pre-population job you can overcome the cold files when users logging in in the morning.

Note: One of the requirements for this model is that local stand-alone namespace "**Random Order**" (rather than "**Lowest Cost**") distributes the users across multiple edge instance instead of having user**A** to user**E** use Edge1, userF to userJ use Edge2, etc.

Stand-alone DFS Namespace should be configured as follows:

Namespace: `\\Edge[X]\CentralData\`

(Random when using Round-Robin)

Folder: Talon

Referrals:

- `\\Edge1\FASTData\Talon`
- `\\Edge2\FASTData\Talon`
- `\\Edge3\FASTData\Talon`

© 2020 NetApp, Inc. All Rights Reserved.

Figure 14)

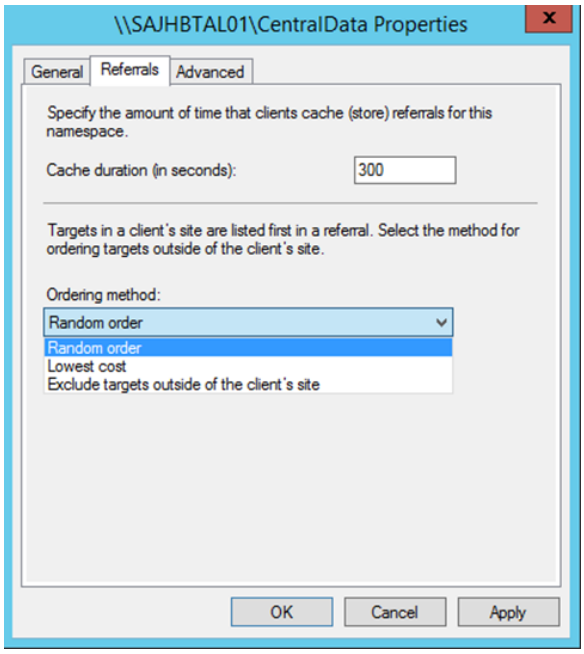
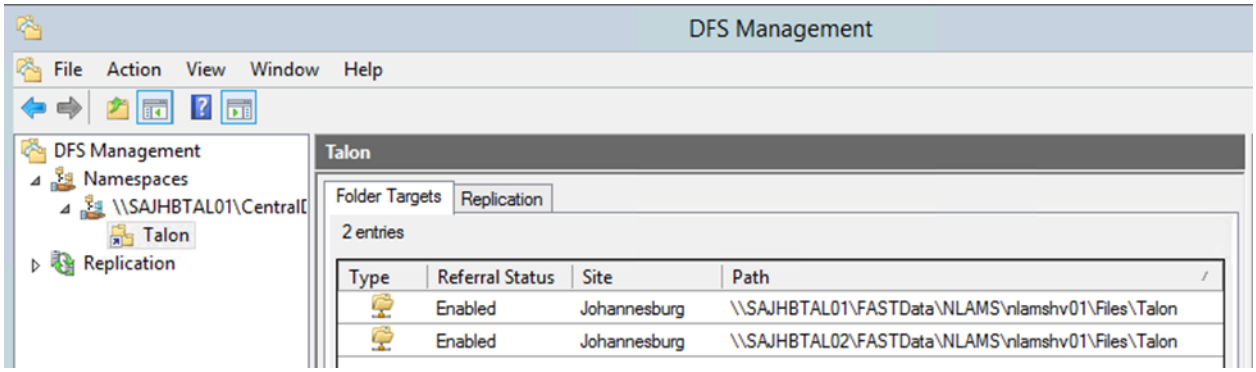


Figure 15)



Domain-Based DFS Namespace

The primary Stand-alone DFS target (`\\Edge1\CentralData\Talon\FS1\Share\Folder`) can then be added to the domain-based DFS namespace structure, which will subsequently resolve to the site where both end users and multiple edge instances reside in. For the Domain-Based DFS namespace it's important "**Exclude targets outside the client side**" is enabled on the DFS folder to reduce the list of feasible targets for a specific client workstation and its partition knowledge table to which the DFS-N resolves.

E.g. `\\domain.local\MFS\Share\` is defined as a folder in the Domain-Based DFS- namespace, using the following referral(s):

- `\\Edge1\CentralData\Talon\FS1\Share (enabled)`
- `\\Edge2\CentralData\Talon\FS1\Share (enabled)`
- `\\Edge3\CentralData\Talon\FS1\Share (enabled)`
- `\\FIleServer\FS1\Share (last among all targets) <- native target`

© 2020 NetApp, Inc. All Rights Reserved.

Figure 16)

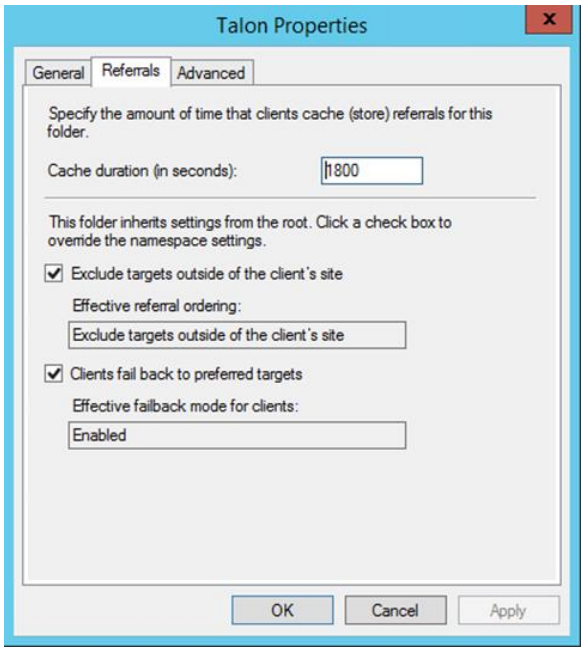
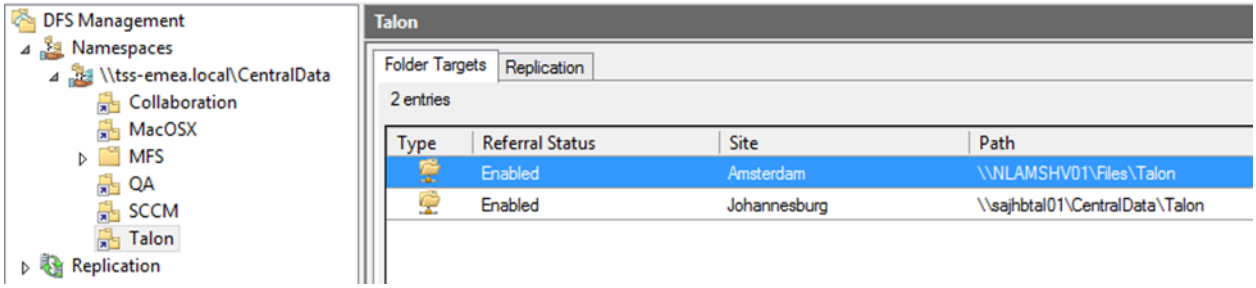


Figure 17)



© 2020 NetApp, Inc. All Rights Reserved.

Redundancy Options

For the purpose of redundancy, you can add the same standalone configuration to Edge2 and Edge3 and integrate them as referrals in the Domain-Based DFS-Namespace. Because each edge instance contains the 'same' local stand-alone DFS namespace, the users will enumerate the 'nearest' or preferred stand-alone DFS namespace server, i.e. `\\Edge1\CentralData\Talon\FS1\Share` which subsequently points to `\\Edge1\FASTData\Talon\FS1\Share or \\Edge2\FASTData\Talon\FS1\Share` if the user limit is exceeded.

In a nutshell, the local user maps to the Domain-Based DFS namespace, which has a referral to the local stand-alone DFS namespace, the local DFS namespace uses round-robin to distribute the users between all available edges, subsequently presenting the local edge FASTData virtual file share to the users.

In case of a full site outage, when all Edge instances in a respective site are down, the client will enumerate the `\\BackendFileServer\FS1\Share` target as “last among all targets” referral and point users directly to the backend file server in the datacenter.

Note: For more details relating to DFS Namespace refer to Section 9 of this user guide

© 2020 NetApp, Inc. All Rights Reserved.

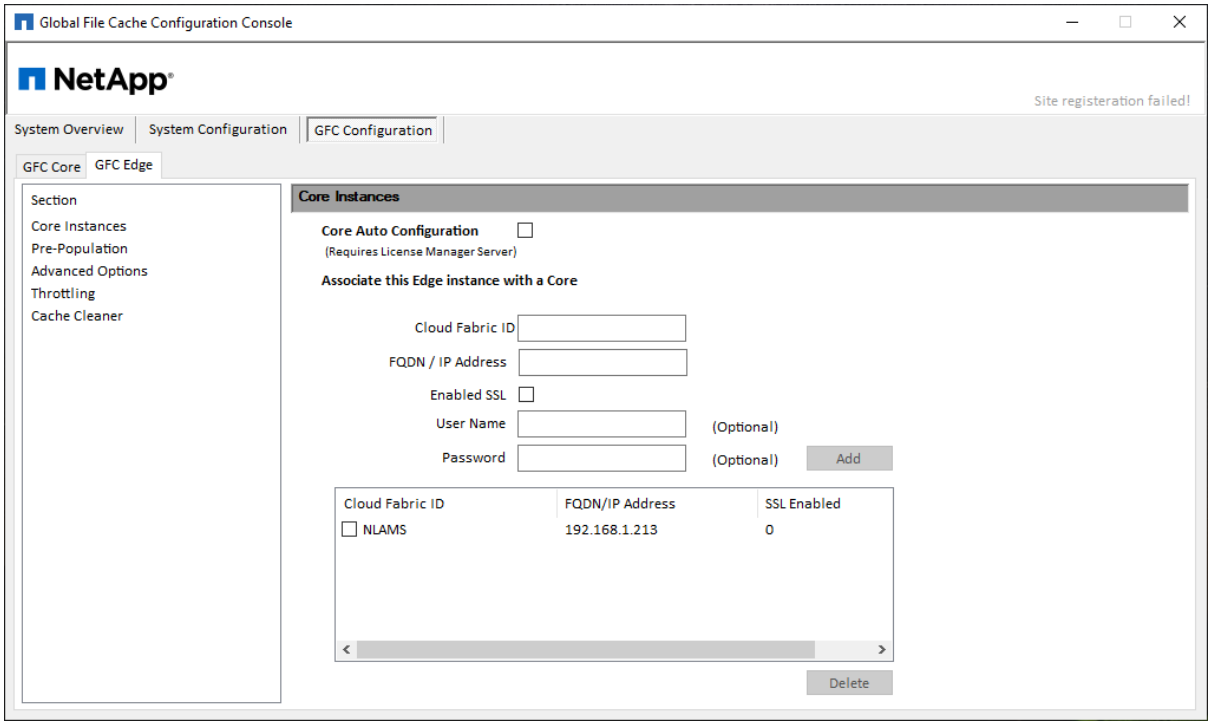
8.3 Configuring the GFC Edge Role

Note: The Edge instance must be licensed prior to beginning the configuration. For more information on licensing, see “Registering your Core or Edge instance with GFC LMS.”

When a GFC instance is designated the Edge role, it will connect to a GFC Core to provide users at the branch office access to datacenter file server resources.

To configure the Edge Instance Role:

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



© 2020 NetApp, Inc. All Rights Reserved.

8.4 GFC Edge Advanced Features

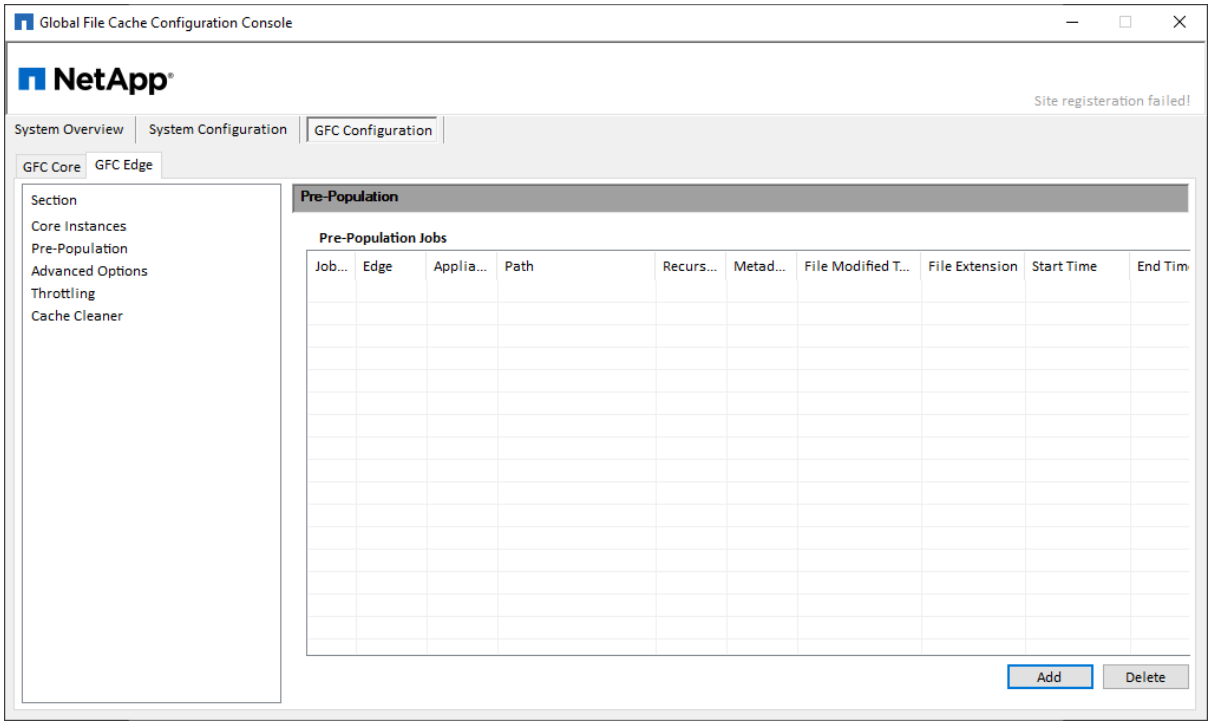
Based on the specific requirements, the Edge instances should be configured the same to maintain consistency within large scale deployments. There specific parameters than can be set on a per Edge base for example, ‘Cache Cleaner’ can vary from site or edge instances.

Edge Pre-population

Note: Please see the latest Release Notes on the GFC website for additional information on GFC Edge Pre-Population.

One-time or recurring pre-population jobs can be configured on an Edge instance.

Figure 18)



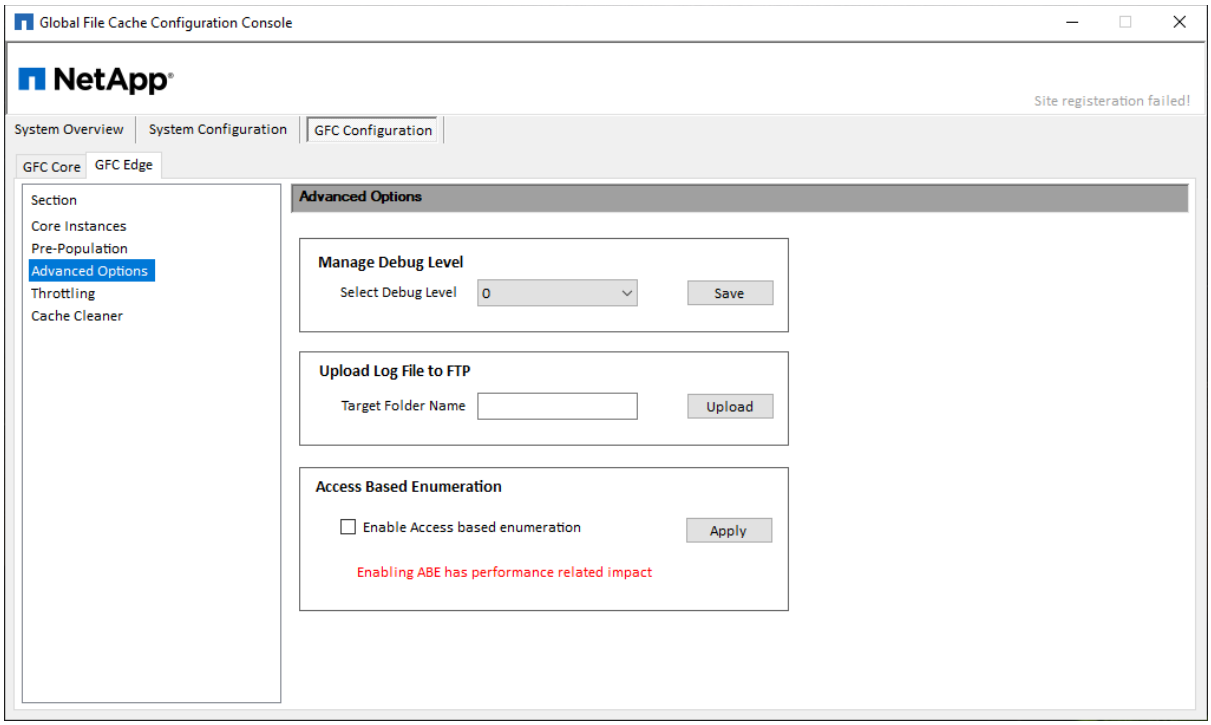
For more information, refer to the “Core Pre-population” section of this document.

Note: The PowerShell Pre-population mechanism is only available from the Core instance.

© 2020 NetApp, Inc. All Rights Reserved.

Edge Advanced Options

Figure 19)



Manage Debug Level

This feature allows for more verbose (higher numbers, MAX: 9) debug logging.

Upload Log File to FTP

This feature enables a direct transfer of requested log files to NetApp Support.

Access Based Enumeration

This feature enables access-based enumeration on the FASTData Virtual File Share on the GFC Edge. Access Based Enumeration (ABE) allows you to hide specific files and folders for user who don't have access permission.

1. To enable access-based enumeration, check the respective check box.
2. Click "Apply," confirm that ABE has been enabled by browsing through the Virtual File Share \\EdgeServer\FASTData\FabricID\BackendFileServer\ from a workstation in the same site using a non-administrative account.

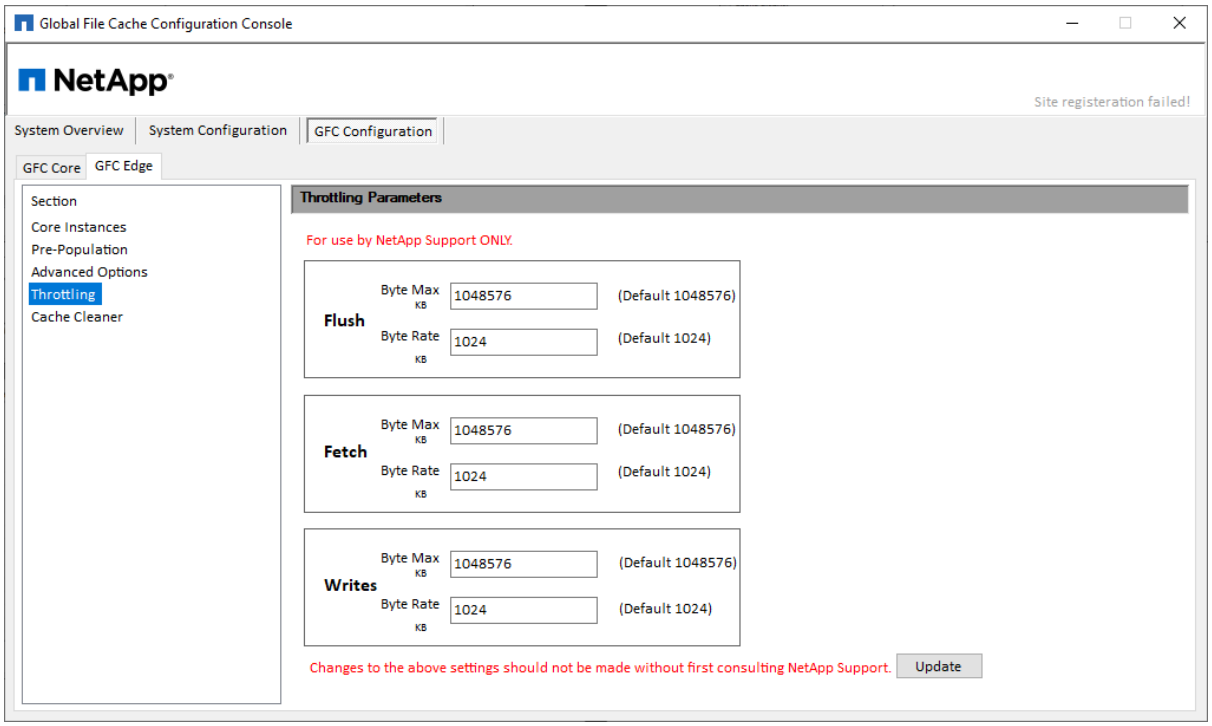
   Note: A reboot may be required to enforce ABE on the GFC Edge.

Throttling Feature

GFC enables specific controls over user behaviors when interacting with their local GFC Intelligent File Cache and Virtual File Share. The advanced Throttling options are set by default and should only be modified after discussing the current user workflow and behavior and consulting on these items with a member of NetApp Support.

© 2020 NetApp, Inc. All Rights Reserved.

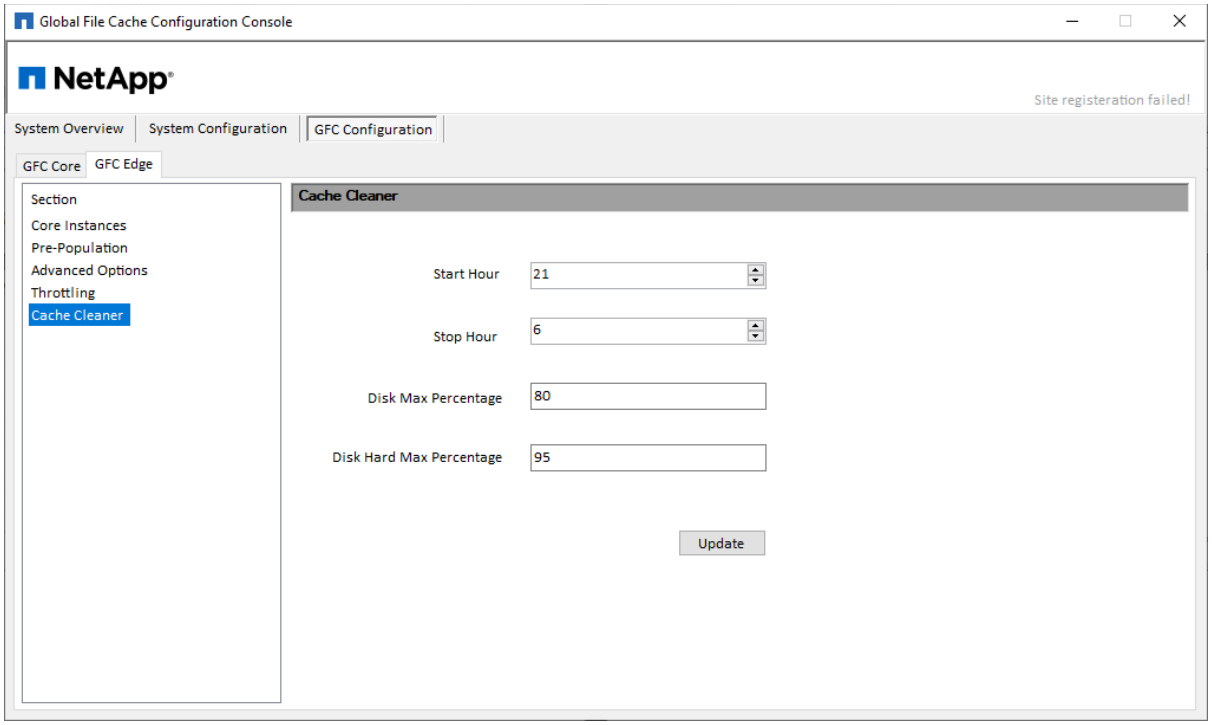
Figure 20)



Cache Cleaner

The GFC Edge Cache Cleaner mechanism can be adjusted to a specific behavior to meet specific time frames or low / high percentage thresholds.

Figure 21)



© 2020 NetApp, Inc. All Rights Reserved.

Start Hour / Stop Hour

The GFC Cache Cleaner mechanism is scheduled to begin at the specified hour (24hr clock) in the local time zone when the **Disk Max Percentage** has been reached. If a **Stop Hour** time is set, the Cache Cleaner will complete the cleaning of the current item and stop afterwards. The default setting is set to 9PM local time (21:00) and will run until 6AM the following morning (06:00).

Disk Max Percentage

This number (1-100) will signal to the Cache Cleaner at what percentage of cache disk utilization to schedule the Cache Cleaning process depending on the specified **Start Hour** as shown above. This percentage may vary among differently sized cache volumes across Edges. The default setting is 80% of the cache volume capacity.

Disk Hard Max Percentage

This number (1-100) will signal to the Cache Cleaner at what percentage of cache disk utilization to immediately begin the Cache Cleaning process. This is a very resource intensive process and may degrade user performance if it occurs during working hours. This percentage should be high enough to allow users to cache new data if the **Disk Max Percentage** value is reached but low enough where users will not be able to completely fill the cache volume. The default setting is 95% of the cache volume capacity.

Note: Depending on the age of the data, the purging of the cache will clean up 25-75% of stale cached data.

Note: To run a manual Cache Cleaner process, refer to the PowerShell Appendix C.

© 2020 NetApp, Inc. All Rights Reserved.

9 DFS Namespace Integration

Distributed File System (DFS) allows administrators to group shared folders located on different servers by transparently connecting them to one or more DFS namespaces. A DFS namespace is a virtual view of shared folders in an organization. Using the DFS tools, an administrator selects which shared folders to present in the namespace, designs the hierarchy in which those folders appear, and determines the names that the shared folders show in the namespace.

When a user views the namespace, the folders appear to reside on a single, high-capacity hard disk. Users can navigate the namespace without needing to know the server names or shared folders hosting the data. DFS also provides many other benefits, including fault tolerance and load-sharing capabilities, making it ideal for all types of organizations.

DFS namespace allows customers to present a 'single pane of glass' to their end users, regardless of the location they're in. The intelligence of Active Directory Sites and Services and client workstation's Partition Knowledge Table (PKT) allows the users to transparently access their centralized data through the 'nearest' NetApp Global File Cache (GFC) caching instance in their site and allow for failover to the 'native' central target in case of a local branch office outage.

More information on DFS: https://technet.microsoft.com/en-us/library/cc782417(v=ws.10).aspx

9.1 DFS Design

The Microsoft Distributed File System (DFS) is a set of client and server services that allow a large enterprise to organize many distributed Server Message Block (SMB) file shares into a distributed file system. DFS provides location transparency and redundancy to improve data availability in the event of failure or heavy load by allowing shares in multiple locations to be logically grouped under one folder or DFS root. This can be configured in a domain-based or standalone configuration.

i.e. `\\corporate.local\root\share\folder`

Direct Share Mapping

Clients are given network-path mapped drives, which connect directly to the Edge appliance cache. This is usually done with a UNC path of the client folder, for example:

i.e. `\\<` GFC `edge>\<FASTData>\<FAST Fabric ID>\<file server>\<share>\<folder`

Configure Windows Server 2016 or 2019 Domain-Based DFS for GFC

Objectives:

- Provide a unified namespace solution for both GFC Cached file/folder structures.
- Introduce Client-side referral-based failover/failback solution based on Windows PKT info.
- Exclude ANY other targets from the Windows Client referral list.

9.2 Site Definitions and Site Links

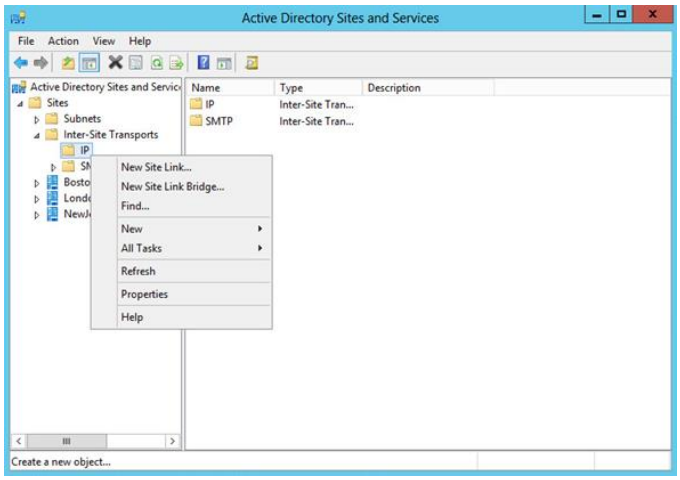
Each Active directory site/subnet must be defined in Active Directory Sites and Services. In order to document the logical network topology, which allows efficient replication of Active Directory; all subnets must be included and linked to a specific site definition.

It is recommended to configure site links based on a star-topology, i.e. Edge1 -> HQ (cost 200), Edge2 -> HQ (cost 500), but include the physical network topology in the design process of configuring Active Directory sites. If no altered Active Directory replication traffic is in place, you can keep the site costs the same (200). Site links define the scope of DFS Management target evaluation.

1. Create Site Links: (if more than two sites)

© 2020 NetApp, Inc. All Rights Reserved.

a. Open “Active Directory Sites and Services”

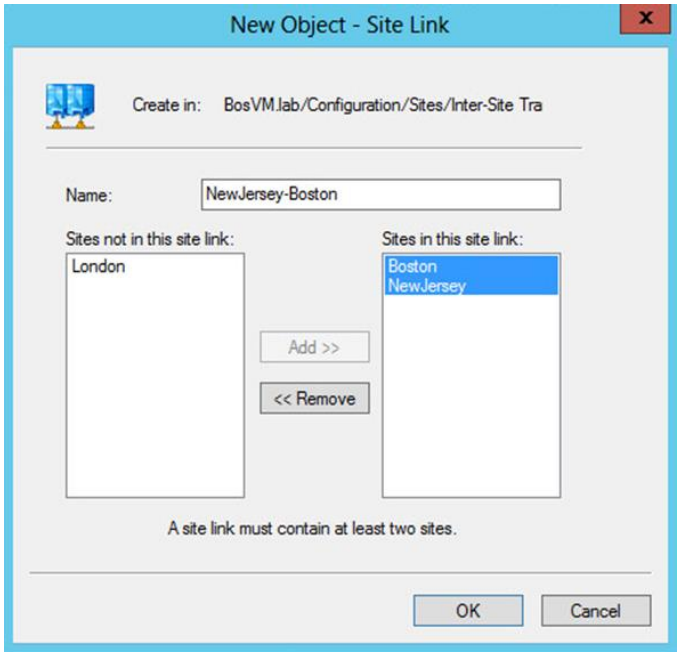


b. Expand “**Inter-Site Transports**”

c. Right click “**IP**“

d. Select “**New Site Link**”

e. Type a name describing which sites will use this link (i.e. NewJersey-Boston)



f. Select sites from “**Sites not in this site link**”

g. Click “**Add**”

h. Click “**OK**”

Repeat steps d-h for each site link that needs to be created.

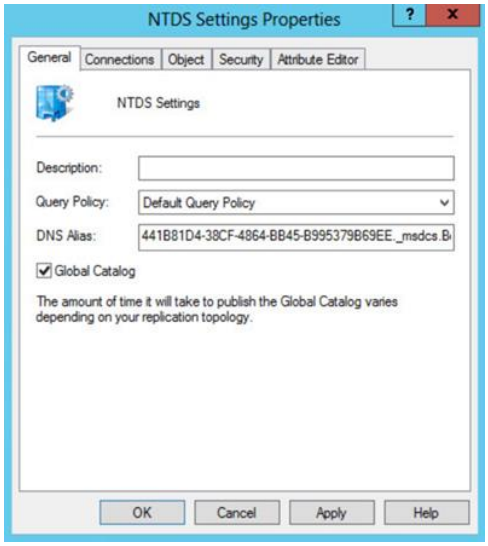
2. Configure “**Query Policy**” and Global Catalog:

a. Double click on a site

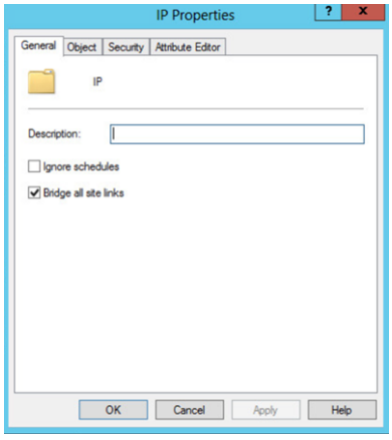
b. Double click “**Servers**”

© 2020 NetApp, Inc. All Rights Reserved.

c. Select available Domain Controller within the site
d. Right click “**NTDS Settings**” and select “Properties”
e. Set the Query Policy to “**Default Query Policy**”
f. Check “**Global Catalog**”
g. Click “**OK**” to commit the changes



3. Bridge Links:
   a. Return to the main screen and double click “**Inter-Site Transports**”
   b. Right click “**IP**” and select “**Properties**”
   c. Confirm “**Bridge all site links**” is checked.
      If it is not checked, closest site selection will fail.
   d. Click “**OK**” to commit the changes.
   e. Close “**Active Directory Sites and Services**”



9.3 DFS Root Configuration Default

A domain-Based DFS root namespace includes all sites based on Lowest Cost, which can introduce issues in terms of client failover. In DFS Management you can configure target failover solution based on

© 2020 NetApp, Inc. All Rights Reserved.

"**Exclude Targets outside of Clients site**" to circumvent that scenario. For each namespace, configure "**Allow Client Failback**." Please follow the steps below to complete the DFS configuration.

If you manage the DFS root from a Windows Server instance, you can generate the following structure as follows. In the exhibit below we are using "`\\BosVM.Lab\DFSroot`" as a namespace, and "TalonFAST" as a target referral.

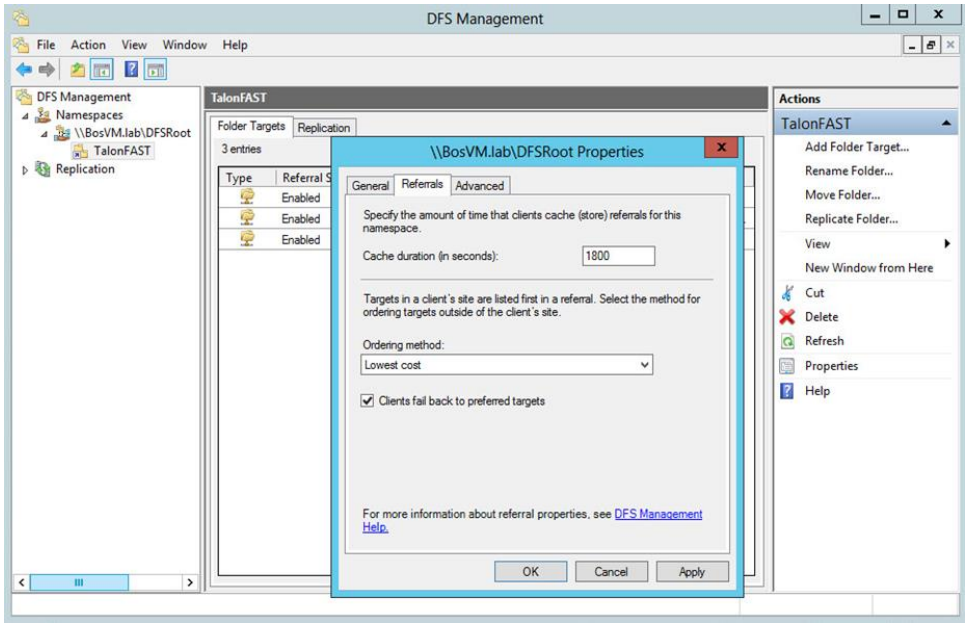
1. **Install the DFS management snap-in**

   The DFS Management snap-in has been included since Windows Server 2003 R2 and allows extensive configuration of a DFS infrastructure. In order to comply with GFC best practices you should use the management snap-in. This is installed while adding the DFS Namespaces role via the Windows Server 2016 or 2019 "**Add Roles and Features Wizard**" found in the Server Manager console.

   More information on installing DFS can be found at

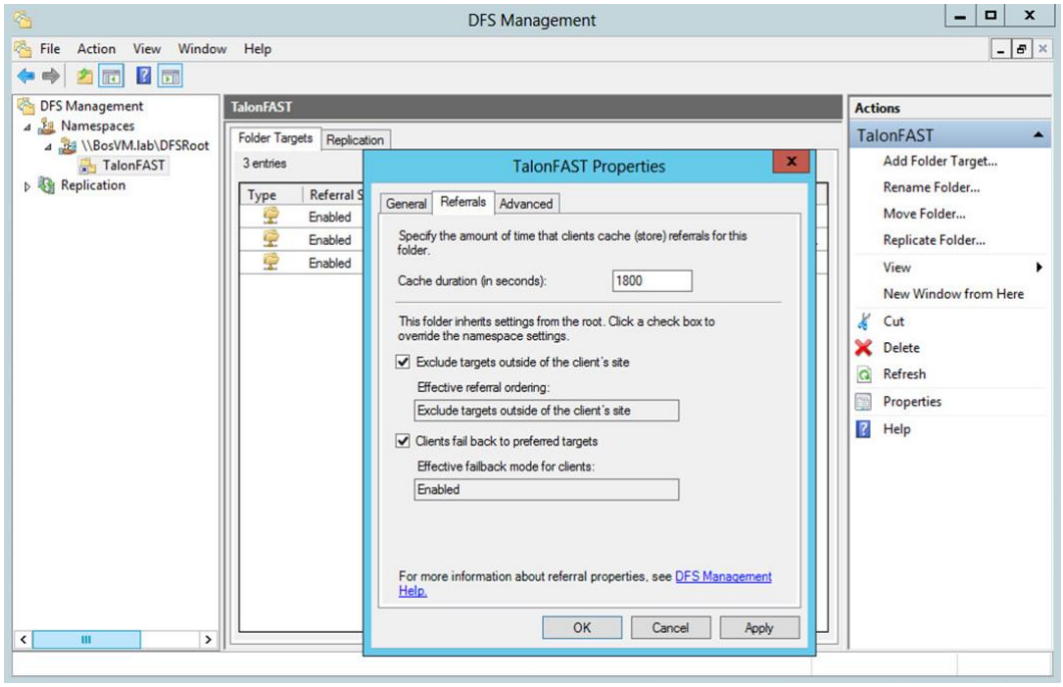
   https://msdn.microsoft.com/en-us/library/cc731089.aspx?f=255&MSPPError=-2147217396#BKMK_UI

2. **Configure the DFS namespace as follows**
   a. Right-click the Namespace **"\\BosVM.lab\DFSroot"** and click "**Properties**".
   b. On the Referrals tab, set the "**Cache Duration**" to 1800 seconds.
   c. Set the Ordering Method dropdown to "**Lowest Cost**".
   d. Check the box "**Clients fail back to preferred targets**".
   e. Click "**OK**" to confirm the configuration change.



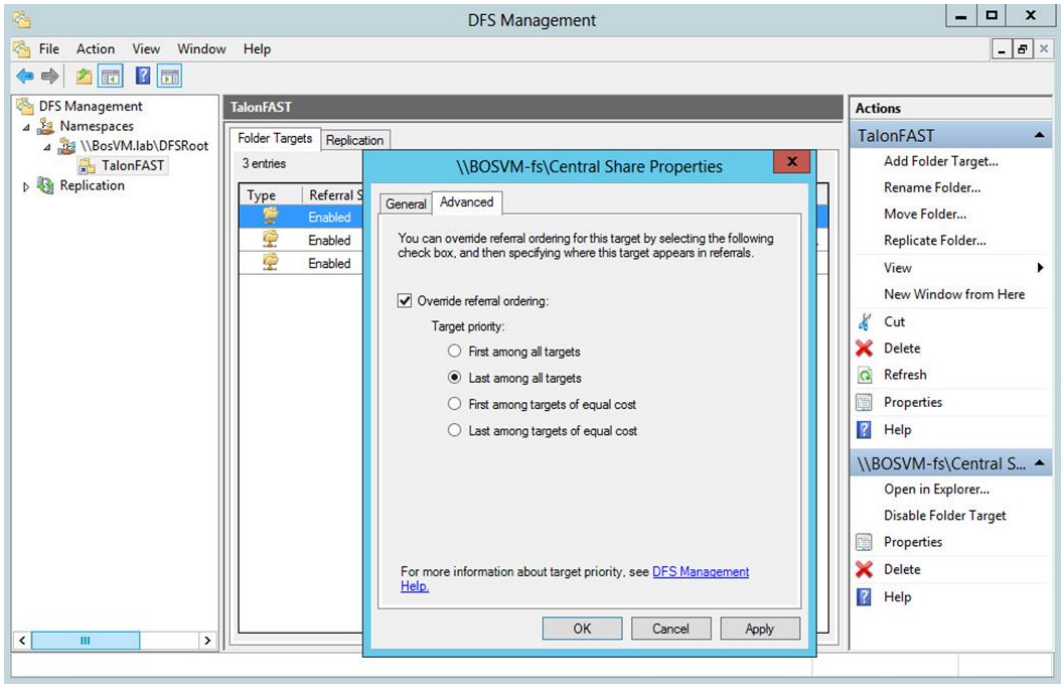
3. **Configure the DFS referral to exclude any target references**
   a. Right-click the referral and select "**Properties**".
   b. For the reference, check the box for "**Exclude targets outside of the client's site**" and "**Clients Failback to preferred targets**".
   c. Set the "**Cache duration**" to 1800 seconds.
   d. Click "**OK**" to confirm the configuration change.

© 2020 NetApp, Inc. All Rights Reserved.



4. **Open the Target Referrals listed in the root folder referral list.**
   a. Right-click the native backend referral, and click “**Properties**”.
   b. Click the “**Advanced**” tab and check the "**Override referral ordering**" box and change the priority to "**Last among all targets**".
   c. Click “**OK**” to confirm the configuration change.
   d. For each GFC Edge referral, right-click the referral, select “**Properties**,” enter the Advanced tab, and ensure that the "**Override**" setting for referral ordering is unchecked.

      Click “**OK**” to confirm the configuration change.



© 2020 NetApp, Inc. All Rights Reserved.

Repeat steps 3 and 4 for each referral and target referral list in the namespace.

Make sure that your target referral list contains the FQDN of the referral path.

With the above settings, Windows XP SP2, Vista, 7, or 8 clients will only receive the local GFC edge and the native back-end file server referral in its "**DFS Tab**" or Partition Knowledge Table (PKT).

5. **Final Steps**

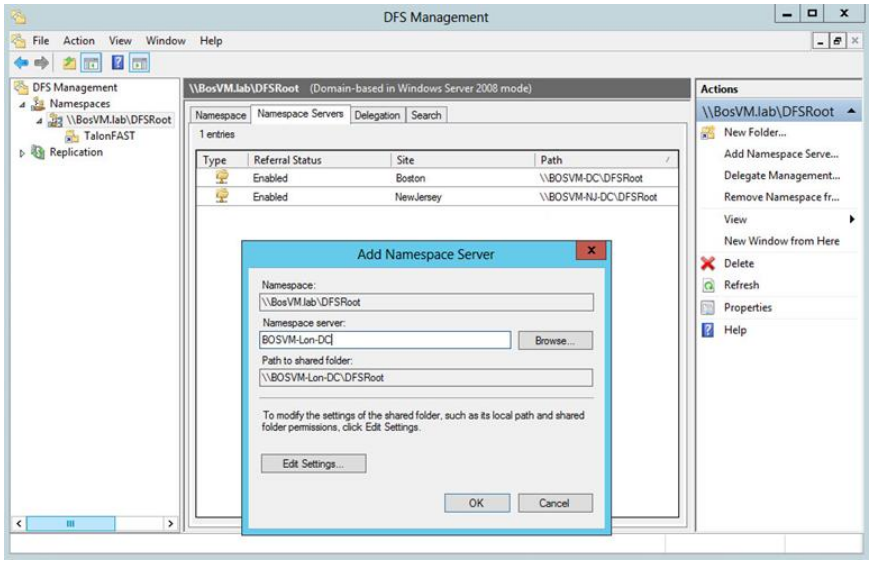
   In order to complete the configuration of a distributed Domain-Based DFS infrastructure, create a replica of the namespace on each domain controller. By creating a local namespace replica, you will increase file system operations performance, as the clients will use their local domain controller. Completing the steps below can be done remotely, from any Windows Server or client, using the DFS Management console:

   a. Right-Click the "`\\BosVM.lab\DFSroot`" namespace.

   b. Click "**Add Namespace Server**".

   c. Select the Domain Controller which will host a replica of the DFS root.

   d. Complete the steps in order to create a DFS root replica on each Domain Controller.



Conclusion:

By using the FQDN as a UNC path, you will introduce a unified namespace and failover solutions for all users in your enterprise network. This simplifies the process of managing data structures, collaborating data between users, and mapping drives on Microsoft Windows clients.

By utilizing a Domain-Based DFS root, using "**Exclude Targets outside of Clients site**" functionality for the target referral, in conjunction with the "**Client-Side Target Failback**" script, you will be guaranteed proper failover/failback operations. Microsoft Clients will never failover to any unwanted path.

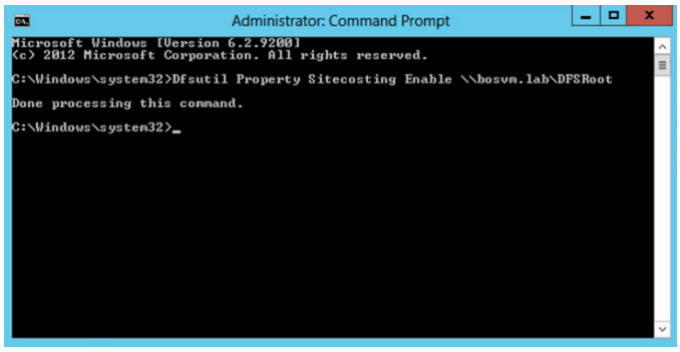
9.4 Site Costing Configuration

For closest site selection to work on link targets, Inter-site Topology Generator (ISTG) must be running on Windows Server, and for closest site selection to work on link and root targets, all domain controllers must be running Windows Server 2016 or 2019. Please use DFSUTIL.exe from the command line to enable site costing:

Windows Server 2016 or 2019: Dfsutil Property Sitecosting Enable \\bosvm.lab\DFSroot.

© 2020 NetApp, Inc. All Rights Reserved.

Figure 22)



Domain Controller (DC) site costing is controlled separately on each DC using the following registry key:

HKLM\System\CurrentControlSet\Services\Dfs\Parameters\SiteCostedReferrals

DWORD 1 or 0

Please validate that the registry entry is applied and schedule a reboot of the respective DC.

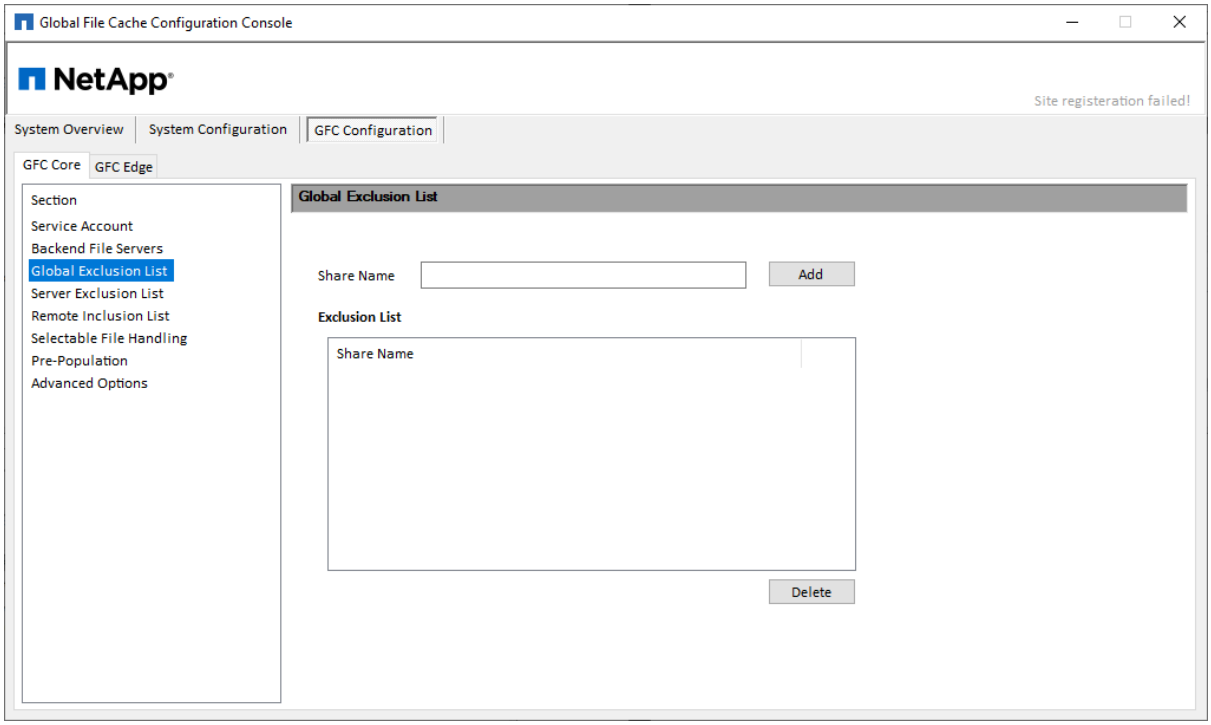
9.5 GFC Global Exclusion Configuration (DFS)

When the DFS root is being hosted by the same backed file server that you are configuring for optimization with GFC, it is recommended that you exclude the local DFS root share from being advertised.

For example, if the **"\\BosVM.lab\DFSroot**" DFS root is being hosted on Fileserver1, and Fileserver1 is also a server that you are advertising through GFC, you should exclude the "**DFSroot**" share.

This can be adjusted in the "**Global Exclusion List**" configuration on the GFC Core configuration page.

Figure 23)



© 2020 NetApp, Inc. All Rights Reserved.

Note: Using a DFS root as your backend file server is not recommended and can lead to data loss.

© 2020 NetApp, Inc. All Rights Reserved.

10 Central Monitoring using Microsoft SCOM

NetApp Global File Cache (GFC) supports integration with Microsoft Systems Center Operations Manager (SCOM) in order to manage different aspects around the solution and integration with Microsoft Windows Server.

This GFC Management Pack includes the following aspects:

- Operational Management
  Systems level inventory.
  Patch level inventory.
- Availability Management
  Systems Health Status.
  Event Viewer.
  SCOM alerting.

i.e. Key services not running.

- Systems Optimization
  % Cache Utilized.
  Cache Purge alert via SCOM.

Dependencies:

- Windows Server 2016 or 2019.
- Systems Center Operations Manager 2012, 2012 R2 (SP1), 2016.
- Administrative Credentials to manage SCOM Operations Manager Console.
- Systems Center Management Pack for Windows Server Operating System.
- Windows Computer Management Pack.
- GFC.
- Latest GFC Management Pack.

Important: Before installing GFC .mpb file, you have to install "SC Management Pack for Windows Server Operating System.msi" which can be downloaded from, https://www.microsoft.com/en-us/download/details.aspx?id=9296.

Note: If a previously existing management pack is deleted, please wait for 48 hours to re-import the management pack. Otherwise, health rollups may not functional correctly.

For additional information, please visit http://www.vroege.biz/?p=768.

10.1 Deploying GFC SCOM Management Pack

This section describes installing and upgrading the GFC SCOM management pack. You can install or upgrade the GFC SCOM management pack by copying the management pack files to the SCOM server instance and following the steps outlined below.

Download the latest software update from http://www.talonstorage.com/support/downloads

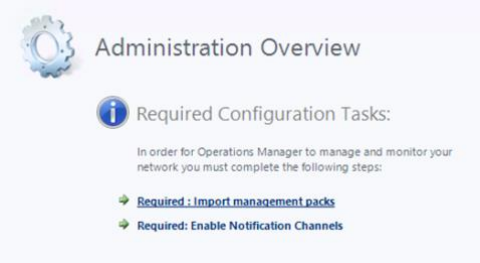
The GFC SCOM management pack includes an .mpb file that needs to be imported within your Microsoft Systems Center Operations Manager 2012 R2 or 2016 Operations Management Console.

In order to implement the management pack, follow these steps:

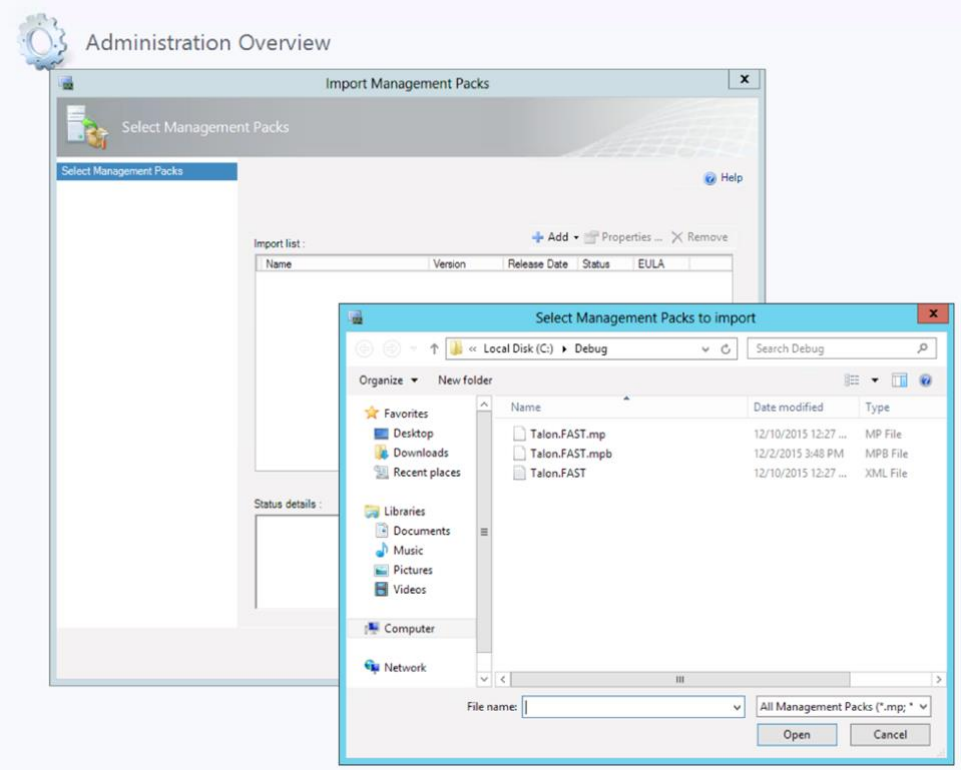
1. Open the Microsoft Operations Management Console.
2. In the left-bottom windowpane, select ”**Administration**”.

© 2020 NetApp, Inc. All Rights Reserved.

3. Within the "**Administration Overview**" section of the management console, select the "**Import Management Packs**" option



4. Select "**Add from Disk**" from the "**Import Management Packs**" console and navigate to the latest management pack file (i.e. Talon.FAST.mpb file)



5. Click "**Open**" to confirm the selection.

© 2020 NetApp, Inc. All Rights Reserved.

6. The management pack will be listed in the "**Import List**" section and will be validated.

   Note: If you are upgrading the GFC SCOM Management Pack, you can commit the upgrade in-place.

7. Once confirmed, the import process will take approx. 10-15 minutes to complete.

10.2 Dashboards and Reports

Talon SCOM Monitoring Console contains the following dashboards and overviews associated with the GFC software. From within the console, select the "**Talon Service Monitoring**" folder. This folder contains all the monitored aspects of the GFC software and is organized as follows:

Talon Service Monitoring

- Service Dashboard
- Service Overview
- Core Instances

Core Servers

Error and Warning Logs

TService Backend Status

TUM Monitoring

GFC Service

GFC Service Alerts

GFC Service Inventory

File Transfer

Event Log

- Edge Instances

Edge Servers

Error and Warning Logs

Total Connected Users

TUM & TAPP Monitoring

Cache Monitoring

Cache Cleaner

Edge Server Cache Disk Free Space

GFC Service

GFC Service Alerts

GFC Service Inventory

- File Transfer

Event Log

10.3 Personalized Views

Microsoft Systems Center Operation Manager provides dashboards and views that can be modified to show or hide the most relevant information for IT administrators. By using this functionality, called

© 2020 NetApp, Inc. All Rights Reserved.

Personalized Views, you can show or hide specific pieces of information such as the Name of the server, if it's in Maintenance Mode, the state of GFC services, etc.

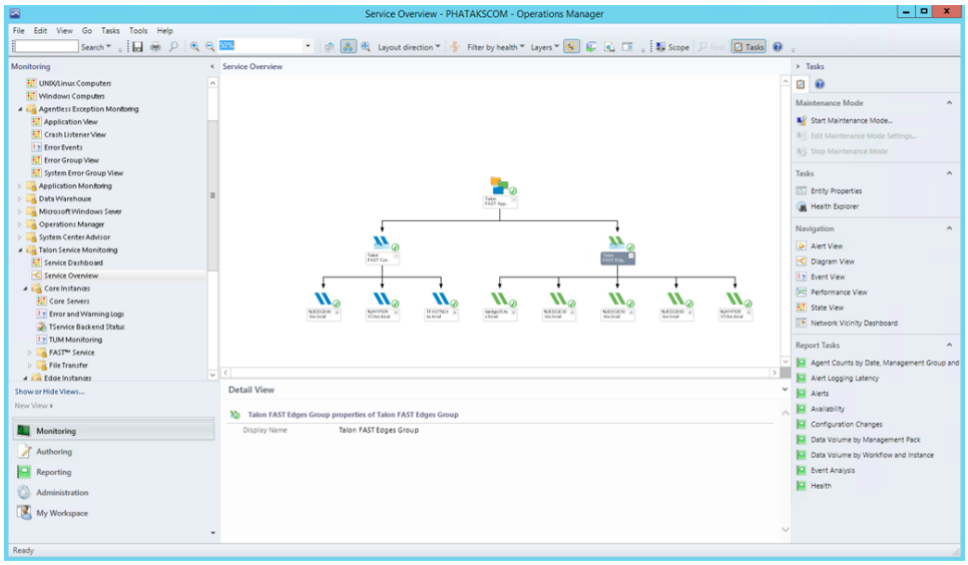
Service Dashboard

The service dashboard contains a list overview of all GFC instances including parameters concerning their health and general configuration. This list includes configuration parameters for both GFC Core and Edge roles.

Service Overview

The service overview contains a logical graphically organized overview of all GFC instances divided into groups of GFC Cores and Edges. This provides users with a high-level overview of the structure and general health of all GFC instances.

Figure 24)



10.4 Core Instances

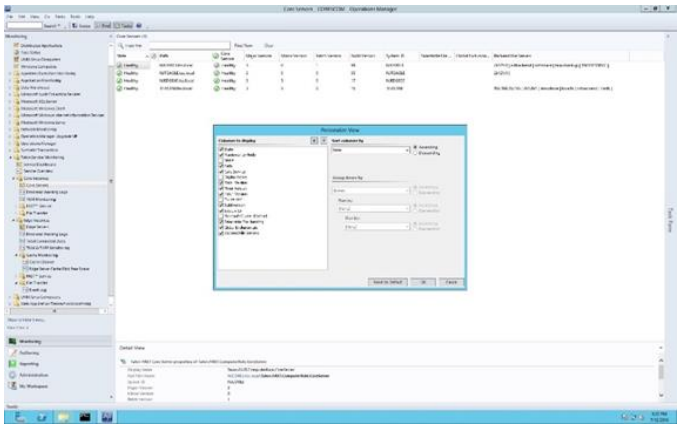
Core Servers

The following information can be enabled through Personalized Views

- State
- Maintenance Mode
- Path – displays FQDN
- Core Service – Running or not
- Major/Minor/Patch/Build Version
- System ID – Displays NetBIOS
- Selectable File Handling (plain text)
- Global Exclusion list (plain text)
- Backend File Servers (plain text separated by pipes " | ")

© 2020 NetApp, Inc. All Rights Reserved.

Figure 25)



Error and Warning Logs

This view contains an extract of logs and warnings from GFC core instances. Including “Event Number” in the Personalized View will help with quickly identifying GFC-specific notifications.

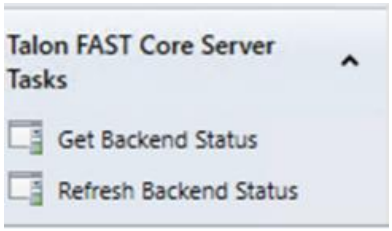
- Level
- Date and Time
- Event Number
- Logging Computer

GFC Backend Status

This contains an overview of tasks initiated by the “GFC Backend Status” Core Server Tasks.

This task can be started from the Core Instances\Core Servers view, which validates privileges and checks permissions on each backend file server associated with the GFC Core instances in the environment.

Figure 26)



TUM Monitoring

This contains an overview of the listed GFC instances and any associated TUM information.

- Level
- Date and Time
- Event Number
- Logging computer

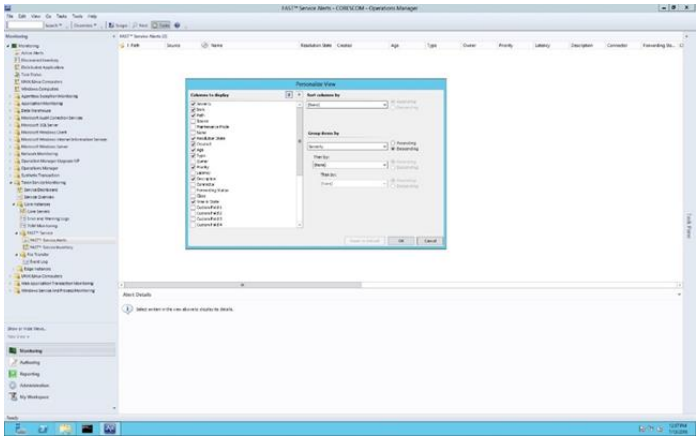
© 2020 NetApp, Inc. All Rights Reserved.

GFC Service Alerts

This contains overview information for all service messages associated with the GFC core role, see Section 10.7 “Event Analysis” for more information.

- Severity
- Icon
- Path
- Resolution State
- Created
- Age
- Type
- Priority
- Description
- Time Resolved
- Time in State
- Time Resolved
- Last State Change
- Site
- Repeat Count

Figure 27)



GFC Service Inventory

This contains an overview of Core Servers, the currently associated Service Account, and the state of the GFC TService.

- State
- Maintenance Mode
- Name
- TService Service Account
- TService Start Mode

© 2020 NetApp, Inc. All Rights Reserved.

File Transfer Event Log

This contains log entries related to GFC File Transfer events. These can be parsed to determine file flushes and fetches.

- Date and Time
- Event Number
- Log Name
- Logging Computer

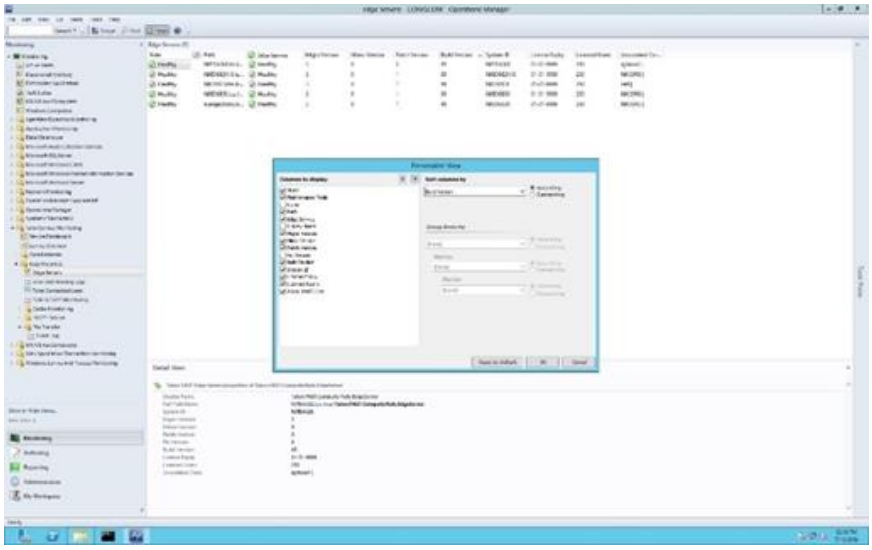
10.5 Edge Instances

Edge Servers

The following information can be enabled through Personalized Views

- State
- Maintenance Mode
- Path – displays FQDN
- Edge Service – Running or not
- Major/Minor/Patch/Build Version
- System ID – Displays NetBIOS
- Licensed Expiry
- Licensed Users
- Associated Cores (plain text separated by pipes " | ")

Figure 28)



Error and Warning Logs

This view contains an extract of logs and warnings from GFC edge instances. Including "Event Number" in the Personalized View will help with quickly identifying GFC-specific notifications.

- Level
- Date and Time

© 2020 NetApp, Inc. All Rights Reserved.

- Event Number
- Logging Computer

Total Connected Users

This view shows all connected Edge servers and statistics of the number of connected users per Edge server currently and over time.

TUM and TAPP Monitoring

This contains Event Log entries in relation to the Edge's TUM and TAPP Processes. This will help with quickly identifying GFC-specific notifications.

- Level
- Date/Time
- Event Number
- Logging Computer

Cache Cleaner

This contains Event log entries in relation to Edge instances' automated cache cleaner mechanism.

- Level
- Date/Time
- Event Number
- Logging Computer

Edge Server Cache Disk Free Space

This view provides a view at each selected Edge server to monitor the amount of available cache space (D:\)

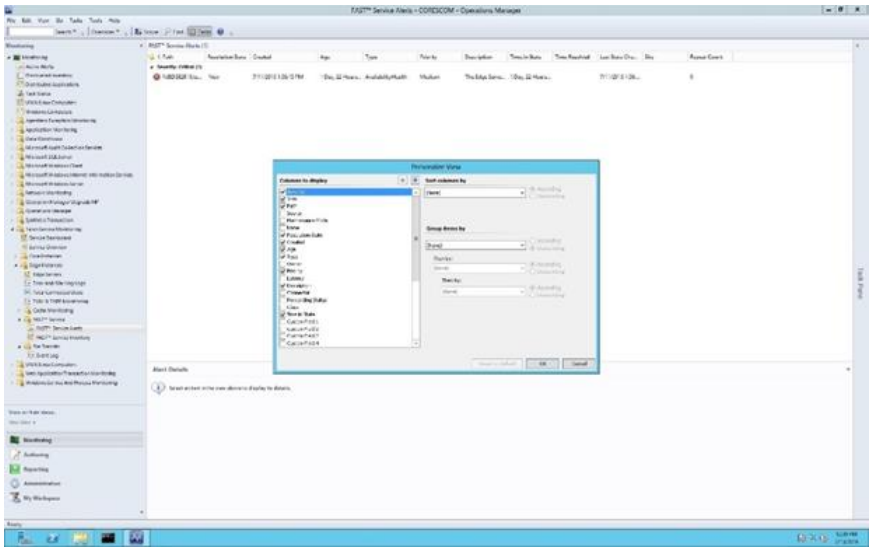
GFC Service Alerts

This contains overview information for all service messages associated with the GFC edge role, see Section 7 "Event Analysis" for more information.

- Severity
- Icon
- Path
- Resolution State
- Created
- Age
- Type
- Priority
- Description
- Time in State
- Time Resolved
- Last State Change
- Site
- Repeat Count

© 2020 NetApp, Inc. All Rights Reserved.

Figure 29)

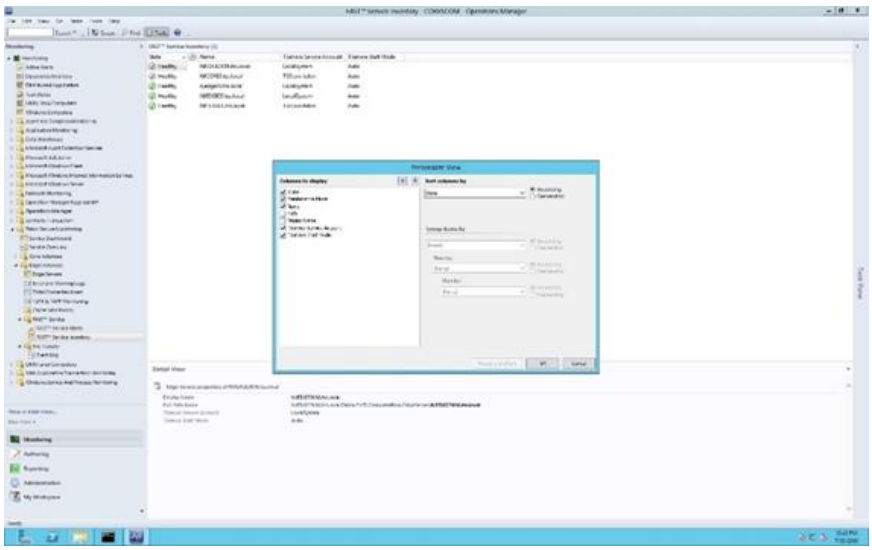


GFC Service Inventory

This contains an overview of Core Servers, the currently associated Service Account, and the state of the GFC TService.

- State
- Maintenance Mode
- Name
- TService Service Account
- TService Start Mode

Figure 30)



File Transfer Event Log

This contains log entries related to GFC File Transfer events. These can be parsed to determine file flushes and fetches.

© 2020 NetApp, Inc. All Rights Reserved.

- Date and Time
- Event Number
- Log Name
- Logging Computer

10.6 Where do I Find?

Below are some commonly asked questions and examples of where to find commonly referenced configurations or informational events and their associated IDs.

Configuration

Identify whether all GFC instances are on the same software version

In the GFC Service Dashboard you can validate the software version using the GFC Major/Minor/Patch/Build Version field names. Once correlated you understand what version you're on, i.e. 3.0.1.99.

Ensure Selectable File Handling has been enabled for specific file types (.SLOG, .accdb, .laccdb)

In the Core Servers dashboard, you can review and verify any Cores and their entries for Selectable File Handling using the Selectable File Handling field name. This will display a text entry for any file extensions associated to the listed Core instances.

Understand number of users connected to my GFC instance

Using the Edge Instances dashboard, an overview of Total Connected Users is presented and displays currently connected users as well as watermarks for user connections over time. Specific Edge instances can be displayed or hidden using the checkboxes in the Performance Counter pane.

Understand the amount of cache space being used on my GFC instance

Using the Edge Instances dashboard, a view for Edge Server Cache Disk Free Space is available to display current disk capacity and utilization levels. Specific Edge instances can be displayed or hidden using the checkboxes in the Performance Counter pane.

Validate my core instance(s) has the correct configuration

In the GFC Core Servers dashboard, you can validate the status of each Core's Core Service, the software version, and the associated backend file servers using the appropriately named fields.

Validate my edge instance(s) are connected to the correct core instances

In the GFC Edge Servers dashboard, you can validate the status of each Edge instance, the software version, and the associated Core Instance using the appropriately named fields.

Functionality

Validate Files are being transferred

All File Transfers can be validated from the Core Instances File Transfer Event Log. This will detail all files fetched and flushed from the backend file server. Edge specific file transfers can be validated and parsed from the Edge Instances File Transfer Event Logs. This allows users to correlate and validate all data fetches and flushes across the GFC environment.

Understand Pre-population Job has started and/or completed

Pre-population job status information can be validated from the Edge Instances TUM & TAPP Monitoring dashboard. Associated Edge instances will list events for both the start and completion of scheduled pre-population jobs.

© 2020 NetApp, Inc. All Rights Reserved.

10.7 Event Analysis

The following Event ID's are commonly utilized throughout a GFC environment. These are provided to allow users to quickly record, monitor, or report on the provided logging statistics from the connected GFC instances.

- 262 – Error on Connection to <IP address>.

Indicator that network connectivity may have been briefly impacted between Edge and Core.

The connections will re-establish automatically.

- 274 (Core) – Connection from <Edge><EdgeIP> successfully established.
- 274 (Edge) – Connections established and authenticate with <Core>.

Connections between Edge and Core have been established successfully.

- 280 – From/To Datacenter (Gathered-Write).

Informational message that data is being read fetched from or flushed to the Datacenter.

This will be visible from the Edge and from the Core.

- 285 – Site key validated for all connections to <Core>. Transitioning to CONNECTED mode.

WAN disconnection resolved, Edge and Core are communicating as normal.

- 287 – Unable to get address for <core>: error 11001 (No such host is known)

Indicates a DNS error where Core cannot be resolved.

- 347 – Transitioning to DISRUPTED mode for <Core>.

Indicates a dropped or lost connecting to the Core. Potentially a WAN error or outage. This should be followed by ID 285.

- 3328 – PrePopulation started at <Time> on <Date> with max_threads 15.
- 3329 – Job is picked up for execution <BackendFS> (Edge).
- 3329 – Job has been completed <BackendFS> (Edge).

Indicates that a Pre-population job has started and completed.

- 282 - Cache Cleaner process is initiated

Automated purging mechanism is engaged.

Indicated cache has reached 85% capacity.

May adjust D:\ accordingly if desired.

10.8 Log Analysis

Finally, GFC uses four sets of files to capture logging on the global file sharing paradigm, which are accessible to the systems and storage administrators via a web-based interface. These files are stored in a structured .TXT text format, to allow both easy viewing for immediate problem determination, or to facilitate export (via .CSV or other formats) to management reporting infrastructures such as SCOM, Splunk, Nagios, Zabbix, etc.

The four areas of GFC management logging are:

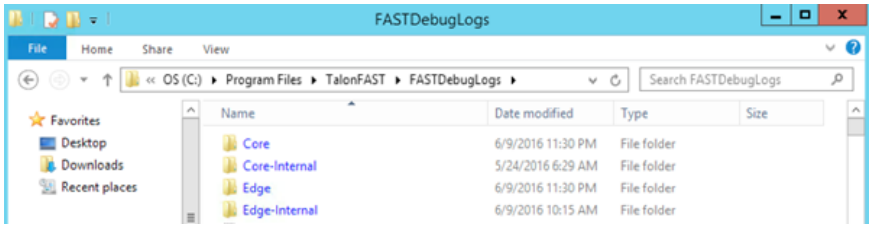
- GFC File Transfer Log
- GFC Message Log
- GFC Stats Log
- TAPP Log

Each of these provides insight into different aspects of the globally consolidated storage environment that GFC enables for customers.

© 2020 NetApp, Inc. All Rights Reserved.

The GFC logs can be found in `C:\Program Files\TalonFAST\FASTDebugLogs\` location on each core or edge instance and collects logs for each role instantiated, i.e. Core or Edge. In addition to traditional logs, a folder can be found that includes Internal information, typically used for support and engineering purposes only.

Figure 31)



GFC File Transfer Log

The logging here provides information regarding files that are handled via the GFC services. Basically, these are files that are either opened on the edge appliance from the datacenter/core, or those that are written to the datacenter core (including updates, saves, copy, and paste type actions). This log allows the administrators to see what files have been accessed (including the full path name), the size of the files, and how well optimized/compressed the actions were. Parameters reported include:

- Date
- Time
- Type of message (Info only, Warning, etc.)
- File path and name
- File size
- Bytes to be transferred (before compression)
- Bytes exchanged over the network (after compression)
- Transfer efficiency (% of data transfer optimized relative to standard file size)

Note: This is higher with uncompressed file types, lower with pre-compressed file types

- User Account SID

GFC Message Log

The GFC Message Log offers insight as to connections over the network between the core and edge appliances, status of licenses in use, as well as general messages. The insight provided includes:

- Date
- Time
- Type of message
- Message text / error descriptor / event descriptor

GFC Statistics Log

The GFC Statistics Log is a static repository in the core/edge which is updated periodically to offer snapshots regarding outstanding connections/leases between the core and edge devices. From the core, the information provided includes:

- Current leases (file locks) outstanding and active
- Updated on a periodic schedule

© 2020 NetApp, Inc. All Rights Reserved.

This information allows a trending analysis, historically, as to the usage patterns of the system globally.

From the edge devices the GFC Statistics Log provides insight as to which core(s) the edge devices are connected to, and the state of that connection (connected vs. disconnected). This information is useful in configuration and availability management for more complex configurations where an edge may be connected to more than one cloud or datacenter core.

TAPP Log

The TAPP Log is used in cases where pre-population (i.e. pre-pop) is part of the configuration or workflow. In order to allow the administrators a high level of confidence that pre-pop has been completed in the time window necessary for workflows (used often in highly complex configurations or often-changing environments), the TAPP Log provides information as to:

- Date
- Time
- Type of message (Info only, error, etc.)
- Message text (file transfer started, file transfer completed, error encountered, etc.)

© 2020 NetApp, Inc. All Rights Reserved.

11 Client Application Best Practices

11.1 Autodesk - Revit

Autodesk Revit users typically work in:

- Revit Stand-alone Project File

Non-collaborative projects are often called “Stand-alone” projects. The project file is available from various locations, but typically used by one user at the time.

- Revit Worksharing Central File

Collaborative projects are worked on with multiple users potentially from multiple sites. This may be in real-time or in a follow-the-sun schedule. A central file of the project is created and all users work across the network on this model. When a user wants to open a central file, the user should be opening the project through the “File” -> “Open” menu in the Revit application. When the central file is opened correctly in this fashion, a copy of the central file is placed locally on the user’s hard drive. There is a link formed between the central, authoritative file and the locally created copy of that central file.

Whenever the user wants to push updates to the central file and update their local copy with any changes in the central file from other collaborating users, they click the “Synchronize with Central” button.

The following application best practices must be adhered to when using the Autodesk Revit application on each NetApp Global File Cache (GFC)-enabled workstation:

- Set the Revit Worksharing Frequency Update timer to Manual intervals
- Users should routinely perform Central File Maintenance on the project to maintain file health (Autodesk Recommendation)
- Before users create new local files through GFC, they should delete or archive/rename their existing local files and their backup folder. More information about this topic and general Revit best practices on Central Files can be found at http://blogs.rand.com/support/2017/04/revit-central-file-maintenance.html

Solving Revit UNC location awareness through a Unified Namespace

In order to use Revit with Worksharing enabled on a central model in a distributed branch office environment, it is required to implement a unified namespace such as a Domain-Based DFS Namespace which provides a unified naming convention for network stored projects and folders.

Adding .SLOG to the GFC Core(s) Selectable File Handling entries – Live Multisite Collaboration

Any Core servers which will be serving Revit files used in a live multisite collaborative situation, must have the .SLOG extension added to their Selectable File Handling entries.

Open Projects via Revit Menus

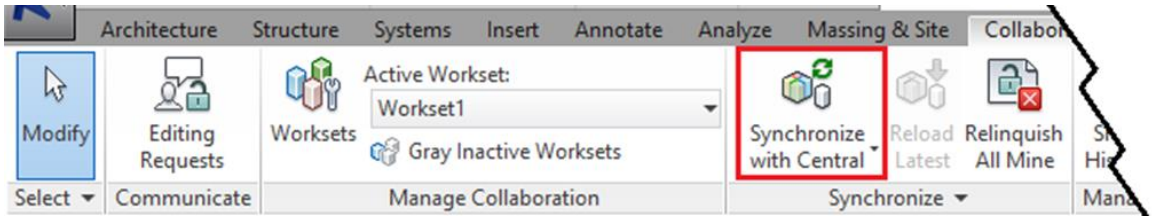
When a user wants to open a central file, the user must first open the Revit application and then the central file though the File -> Open option in the main menu.

Important: Do not open a central Revit file though Windows Explorer (Autodesk Recommendation).

- If the central file is opened correctly, a copy of the central file is created locally on the user’s hard drive. A link is formed between the central file and the user’s local copy of the central file.
- When the project opens, the user is making modifications to their local copy. When the user wants to push updates to the central file and update their local copy with any changes in the central file from other users, they click the “Synchronize with Central” button.

© 2020 NetApp, Inc. All Rights Reserved.

Figure 32)



Note: File saving time depends on number of changes and size of the project.

Borrow Worksets instead of Elements

When users create, add, or adjust single elements, checks are made with the Central Model and the borrowing requests are made to the affected users. When borrowing worksets, all elements of one type are 'owned' by a user and individual elements of that workset must be requested to be borrowed by other users.

Save Often, Sync less

In order to reduce the total amount of data traversing the WAN, GFC recommends that users collaborating on a Revit worksharing project Save their project updates locally and Synchronize with Central less frequently. For example, Save as normal and sync to update other users' changes every few hours. Additionally, when working with a workset or elements, a synchronization will release the ownership which then needs to be regained after the sync completes. By reducing the number of times the central file is checked for updates and ownership of elements and worksets, this will provide an optimal work experience for all live collaborating users.

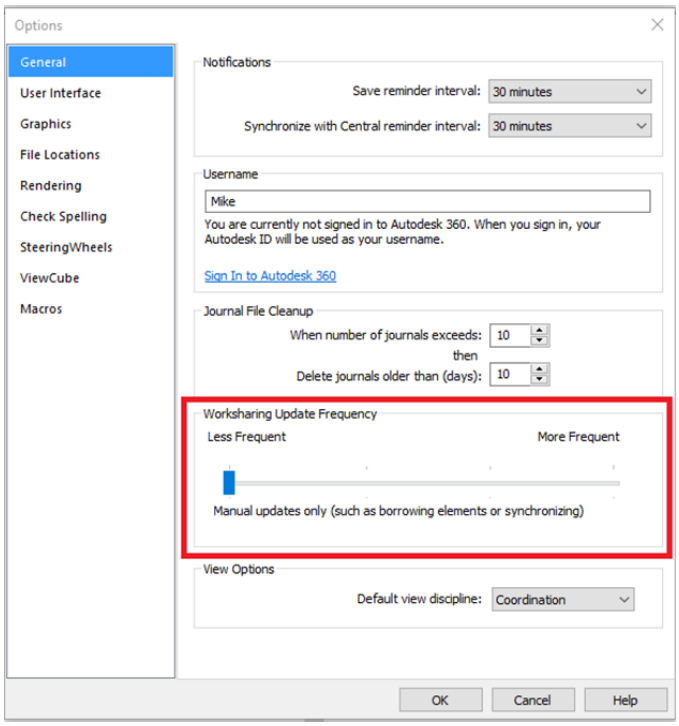
Controlling Worksharing Display Update Frequency in Revit

In Revit, the Central file is used to store the current ownership information for all entities and worksets in the project, and acts as the distribution point for all changes published to the file. When operating in Worksharing mode, users work on a local copy of the Revit model and can save changes to the Central file so that other users can see their work. The local file is the same size as the Central file and can exponentially increase the storage space required for a project when multiple local files are saved on the network. Revit's Worksharing display modes and editing requests are updated in model views and can be adjusted to reduce network traffic.

To change the Worksharing Update Frequency in Revit

© 2020 NetApp, Inc. All Rights Reserved.

Figure 33)



1. Click the logo, and then click "**Options**"
2. In the "**Options**" dialog box, click the "**General**" tab
3. In the "**Worksharing Update Frequency**" area, move the slider all the way to the left for manual updates only. When set to "**manual**," display mode information is only updated when borrowing elements; Worksharing display does not generate network traffic.
4. Click "**OK**"

11.2 Revit Best Practices Summary

Please find below a summary of the Revit Best practices and requirements to ensure that the users will achieve an optimal experience:

1. Always use the global namespace or drive letter to log on specific project before opening Revit
2. Save more often to your local copy (Ctrl+S), synchronize with central model less often (every couple of hours - speak to BIM coordinator)
3. Always communicate with your team members via email or skype messaging whenever needed, do not assume things.
4. In case of issues with files or syncing speak to your BIM Coordinator first, if not available contact BIM Support
5. If Revit file was just created, it takes longer to open such file in overseas office for the first time (depends on RVT file size, in case of 500MB file it can take 30mins)
6. Do not attempt to copy large files from server overseas during work hours. If you do so you might slow network connections between offices and you or other Revit users might not be able to synchronize Revit models.
7. Change Worksharing Update Frequency in Revit from default 5 seconds to Manual to avoid unnecessary network traffic. Ask your BIM Coordinator if you do not know how to do it or consult the full version below.

© 2020 NetApp, Inc. All Rights Reserved.

8. "Accessing Model ..." warning is result of someone else synchronizing with central model at the same time you are trying or GFC synchronizing files between offices. You need to wait for your turn. If it takes too long you need to speak to your local IT Support to check whether network between offices is not 100% busy with some other tasks (see point 7) or whether there is network outage.

11.3 Autodesk - AutoCAD

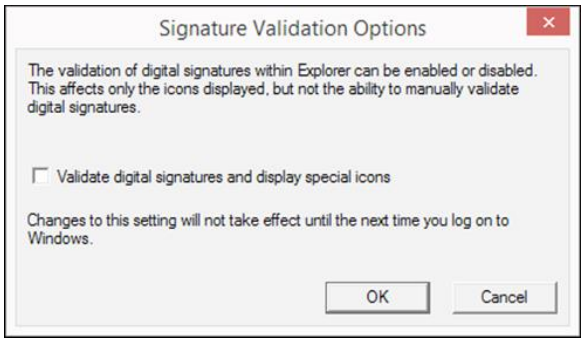
Disable Digital Signatures

Digital signatures contribute to slow browsing of AutoCAD folders and files through GFC instances. For faster browsing, disabling digital signatures is recommended. In 2001, Autodesk introduced Digital Signature Extension, which lets AutoCAD attach digital signatures to any files compatible with the AutoCAD 2000 and later drawing-file formats. In AutoCAD 2004 and all later versions, drawings can be digitally signed directly without using the extension.

During the AutoCAD installation, a shell extension loads displaying a specific icon with the file in Windows Explorer, or in the Open/Save dialog box if it is digitally signed. To determine whether a file is digitally signed, the shell extension scans each drawing file as it is displayed. Folders that contain many drawing files cause this activity to slow the system and decrease productivity.

Disable Digital Signatures (Manual)

1. Use Windows Explorer and navigate to `C:\Windows\System32 directory`.
2. Double-click the "**acsignopt.exe**" file.
   The "**Signature Validation Options**" window displays.



3. De-select "**Validate digital signatures and display special icons**".
4. Click "**OK**".
5. Restart the computer.

Implementing AutoCAD Registry Setting Using AD Group Policies

1. Create a registry file called **autocad.reg** on the desktop.
2. Open the **autocad.reg** file in Notepad and add the following:
   [HKEY_CURRENT_USER\Software\Autodesk\Autodesk Digital Signatures]
   "IconOverlayEnabled"=dword:00000000
3. Save the **autocad.reg** file.
4. Copy the **autocad.reg** file to the logon share.
5. Create a batch file called autocad.bat.
6. Open Notepad and add the entries:
   @echo off

© 2020 NetApp, Inc. All Rights Reserved.

regedit /s \\ServerName\Share\autocad.reg

Save the autocad.bat script in the NETLOGON share on a domain controller at %systemroot%\sysvol\sysvol\<domain_DNS_name>\scripts

7. Start the "**Active Directory Users**" and "**Computers**" snap-in by clicking "Start > Administrative Tools > Active Directory Users and Computers".
8. In the console tree, right-click the local domain and select "Properties".
9. Click the "**Group Policy**" tab, click "New".
10. Type a name for the new policy (for example, AutoCAD Digital Sign), and press Enter
11. Right-click the new policy name, select "**Properties"**.
    a. Click the "**Security**" tab.
    b. De-select the "**Apply Group Policy**" checkbox for the security groups that should not have this policy applied.
    c. Select the "**Apply Group Policy**" checkbox for the groups that should have this policy applied.
    d. Click "**OK**".
12. Click the "**Group Policy**" tab
13. Select the appropriate group policy object (for example, AutoCAD Digital Sign), and click "**Edit**".

    The Group Policy Object Editor displays.
14. Under "**User Configuration**" expand "**Windows Settings**".
15. Click "**Scripts (Logon/Logoff)**".
16. Right-click "**Logon select Properties**." The "**Logon Properties**" window displays.
17. Click "**Add**." The "**Add a Script**" dialog box displays

    Type the full UNC path to the shared folder that contains the script.

    Example:`\\ServerName\SysVol\domain.com\scripts\qq.bat`.

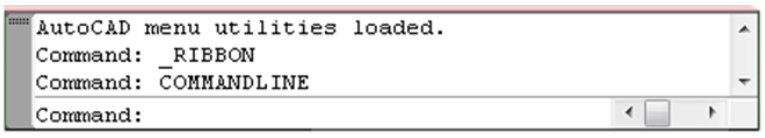
    Note: Do not browse to the location. Use the UNC path to the shared folder.
18. Click "**OK**"
19. Click "**Apply**"
20. Click "**OK**" to close
21. Close the "**Group Policy Object Editor**" Console and the "**Active Directory Users**" and "**Computers**" snap-in. Have all users log out and log back into the domain. The end user PCs now have the following registry setting installed:

    ```
    HKEY_CURRENT_USER\Software\Autodesk\Autodesk Digital Signatures
    "IconOverlayEnabled" =0
    ```

Set AutoCAD Sheet Set Manager Variables

Access and Edit Variables

1. Open the AutoCAD command window.
2. Type the name of the variable followed by the value to set it to.
3. Exit AutoCAD normally to save the new variable value.



© 2020 NetApp, Inc. All Rights Reserved.

Toggle Data Sheet Refresh State

The SSMSHEETSTATUS variable controls how the status data in a sheet set is refreshed.

- Set the SSMSHEETSTATUS variable to 0. The status data in a data sheet does not automatically refresh.

OR

- Set the SSMSHEETSTATUS variable to 2. The status data will be refreshed when the sheet set is loaded or updated.

This setting also indicates that the status data will be refreshed based on the time interval set by SSMPOLLTIME.

Set Data Sheet Refresh Rate Intervals

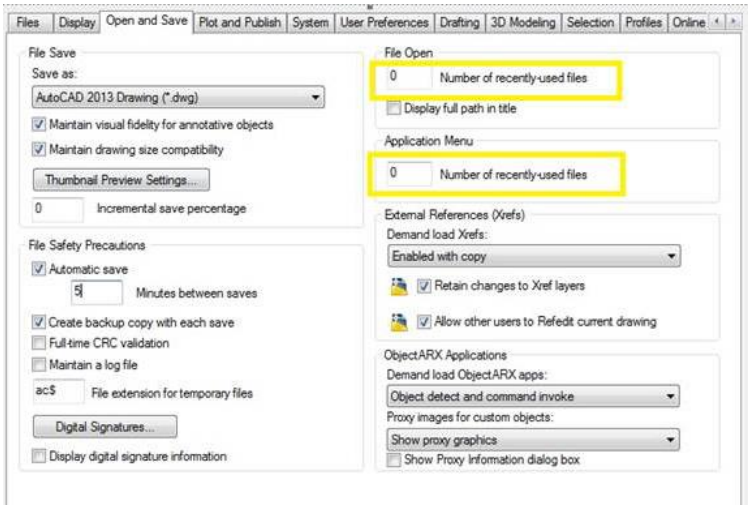
This variable controls the time interval between automatic refreshes of the data sheet status data. The time interval is in seconds and valid values are between 20 and 600. The default value is 60. Set SSMPOLLTIME to 600.

Set XLOADCTL Variable Parameter to 2

This variable controls how xref files are loaded: pre-loaded or on-demand, and if they are locked for exclusive use or a locally sourced copy. Autodesk recommends setting the XLOADCTL variable to 2 to allow for on-demand loading of network resources. If set to 2, copies of xref drawings are loaded and locked, the authoritative xrefs are not locked exclusively.

Turn of File History for recently-used files

To turn File History off, change the Number of recently-used files to 0 for both *File Open* and *Application Menu* items in the “Open and Save” preferences (screenshot below)



Excluding Drawing Files from Antivirus Scanning

Recommendation: Keep AutoCAD drawing (DWG) files excluded from antivirus scans to accelerate the file open and file save processes.

© 2020 NetApp, Inc. All Rights Reserved.

11.4 Bentley – MicroStation

User Preference File (UPF) and Project Configuration file (PCF)

Bentley MicroStation often reads and writes the .UPF and .PCF files in order to update its profile settings. For each user session, the application will write the entire file to the destination location, in this case the GFC server that saves the file to the datacenter. In order to improve application performance, it is recommended to place the .UPF and .PCF files locally on the client, which is MicroStation's default location or on a local share:

```
_USTN_PREFNAMEBASE =
C:\ProgramData\Bentley\MicroStation\WorkSpace\users\Talon\prefs\EYC
```

Disable Auto-Save or Set to Value of 600

Due to the way Bentley MicroStation responds to WAN interruptions, the MicroStation auto-save feature should be disabled and clients should save MicroStation files manually or set this value to 600.

In the event of a network or WAN interruption, MicroStation times out and displays a window that offers the options of retrying or cancelling the save operation. MicroStation does not offer a "Save As" option for files open on client PCs from the data center file server. The retry option causes MicroStation to retry the save operation for 300 seconds or until the network/WAN connection is reestablished, causing the application to appear as if it has frozen.

If a packet arrives during the retry operation, it causes the timer to reset and the operation starts from the beginning. The cancel option causes MicroStation to write the changes to a temporary file and then close. Once the original. dgn file is reopened, the changes are applied to it from the temporary file.

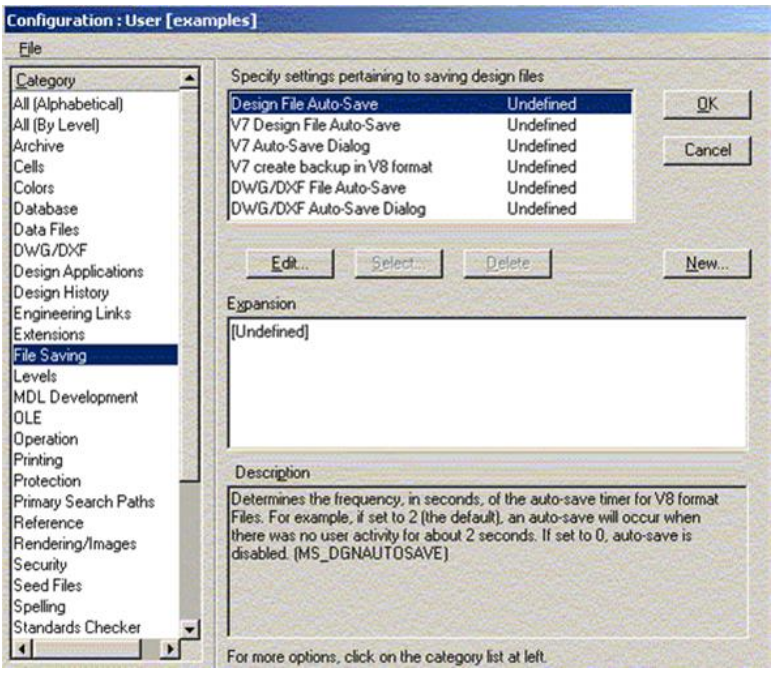
Starting with MicroStation V8 2004 Edition, auto-save can be set up either using configuration files or user preferences. The configuration file technique has the advantage that it can be set up by an administrator for an entire site or workgroup, and it allows more control over how auto-save works. For sites where the auto-save policy is left up to the user, the user preference method can be used. If the auto-save configuration variables are set, they take precedence over the user preference settings.

Adjusting AutoSave settings in Microstation

Under the Workspace Configuration settings, select "**File Saving**." Here users can set auto-save parameters (or review the settings that an administrator has made in site configuration files).

© 2020 NetApp, Inc. All Rights Reserved.

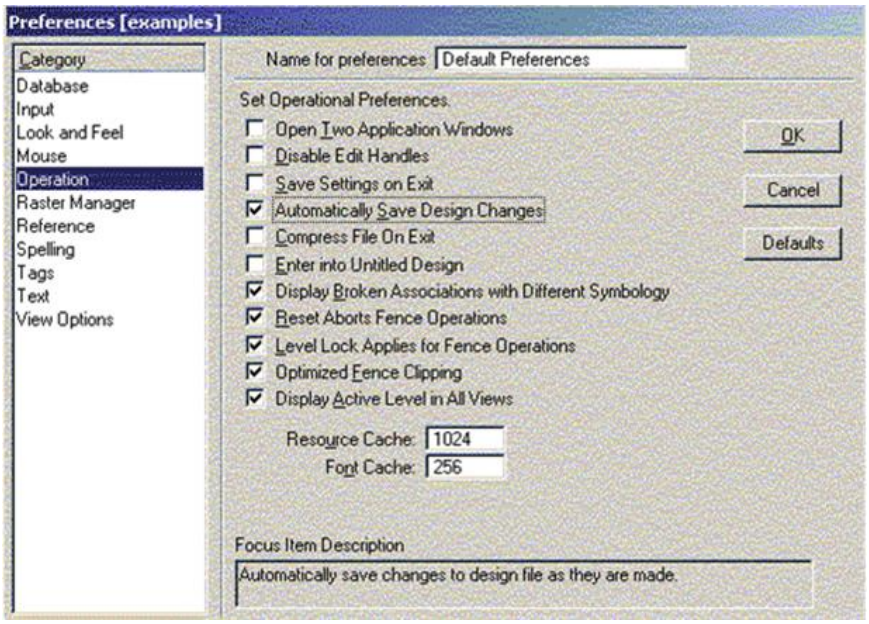
Figure 34)



Setting “**MS_DGNAUTOSAVE**” to 0 will turn off auto-save and prompt the user to save changes when exiting a file. Any other value allows users to set the number of seconds between auto-saves when editing V8 design files. The other configuration variables determine how auto-save works when editing v7 and DWG format files.

If none of the configuration variables have been set, the auto-save user preference determines the behavior. To review or change these settings, go to the “**Workspace > Preference**” pull-down menu and then go to the "Operation" category.

Figure 35)



© 2020 NetApp, Inc. All Rights Reserved.

Check the “**Automatically Save Design Changes**” box (which replaces the Immediately Save Design Changes toggle from previous versions). It is on by default. If any of the File Saving configuration variables are set, the preference is grayed out. Hovering over the preference will indicate that automatic saves are turned on by the **MS_DGNAUTOSAVE** configuration variable or "**Automatic save is turned off because MS_DGNAUTOSAVE is set to 0**.”

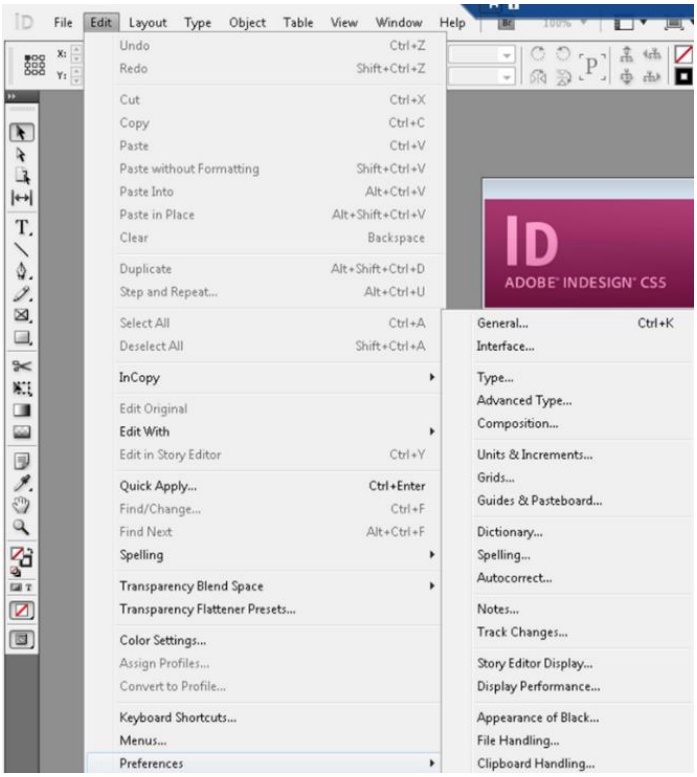
11.5 Adobe Creative Suite

InDesign

To prevent InDesign from checking for links between images within a document and with external documents, it’s recommended to disable checking for links when opening a file. If this is left on, it may result in multiple file read or open operations which may impact performance.

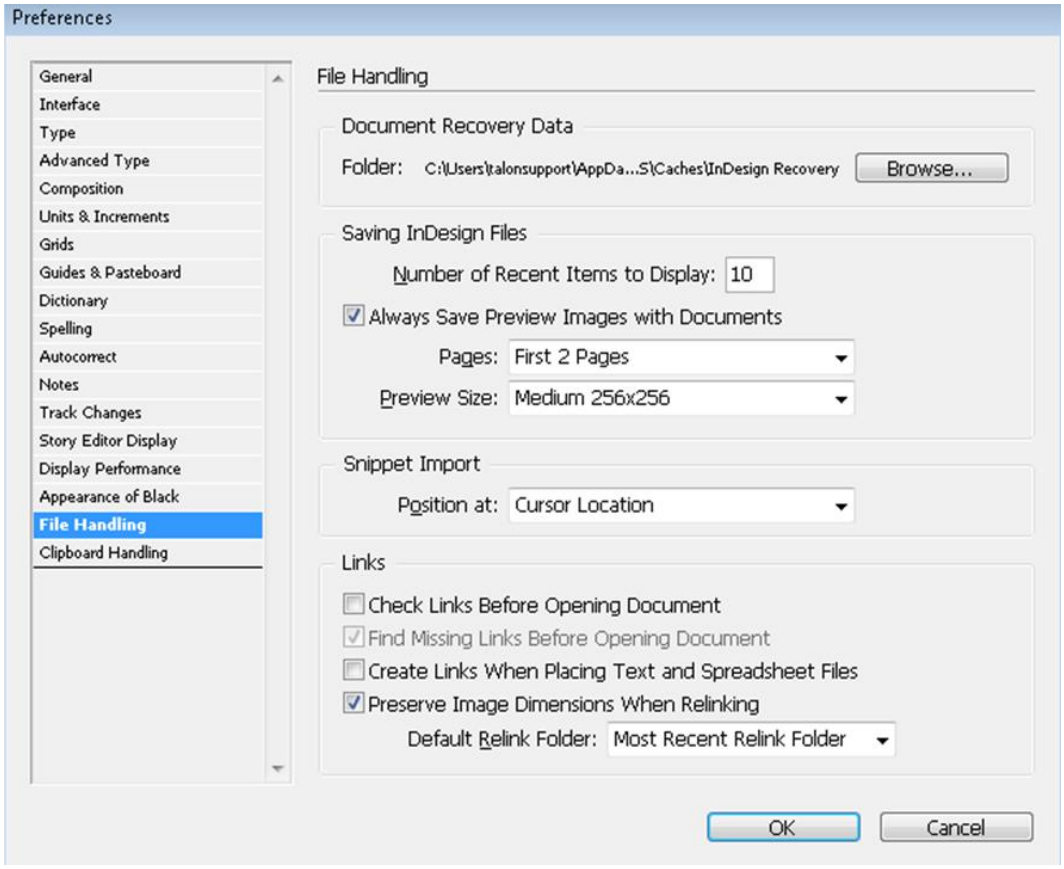
To adjust the link check setting on the client workstation:

1. Click “**File**”.
2. Expand the “**Preferences**” menu.
3. Click “**File Handling**”.



4. Uncheck the box to “**Check links before opening document**”

© 2020 NetApp, Inc. All Rights Reserved.



The Link Check settings can also be adjusted via a script/GPO:

1. Create a new directory named "**Startup Scripts**" at `C:\Users\<username>\AppData\Roaming\Adobe\InDesign\Version11.0\en_US\Scripts.`
2. Create a new JavaScript file within the "**Startup Scripts**" directory with the following contents
   app.linkingPreferences.checkLinksAtIOpen = false;
3. If InDesign is running, close and reopen the application to force the changes to take effect.

Note: This is an optional setting that, depending on the user's workflow, may or may not be feasible.

11.6 Mac OSX Best Practices (10.12 Onwards)

Note: For an optimal experience with Mac OSX clients, GFC recommends to leverage access to the GFC Virtual File Share through AFP (Apple File Protocol). Although SMB/CIFS access is enabled by default, accessible to Mac OSX clients, due to its limitations SMB/CIFS access is supported by GFC on a best-effort basis.

Offline Attribute not Recognized by Mac OSX when Using SMB/CIFS

By default, Mac OSX SMB/CIFS implementation does not support the use of the Offline Attributes on files and folder structures (see also: https://discussions.apple.com/thread/6002286?tstart=0), this means that when browsing through the FASTData file share, cold files (not cached) and metadata objects (i.e. file/folder name, ACLs) are not visible at first. Once browsing into a path structure, a user may need to manually refresh the folder's metadata by right-clicking in the folder and click 'Get Info' for the folder contents to appear.

© 2020 NetApp, Inc. All Rights Reserved.

Recommended Approach: Acronis Files Connect

Acronis Files Connect allows for resharing of the FASTData file share through AFP (Apple File Protocol). This can be enabled by installing the Acronis Files Connect solution on each GFC Edge instance (or Windows Server instance in the same site) and export the local SMB share (\\Edge\FASTData\ ) or a newly-created share nested in \\Edge\FASTData through AFP (preferred).

Subsequently, the ArchiveConnect functionality can be enabled to present 'COLD' folders/files differently than 'WARM' folders, i.e. all 'COLD' objects can be marked a specific color so the user understands the data is cached or not. By using AFP over SMB, the issue with folder refreshes is addressed and less clunky, whilst performance is equivalent when it comes to file open / save operations.

Note: Contact your GFC Solutions Engineer or NetApp Support discuss your requirements.

Disable Indexing of Network Locations (OSX 10.12)

Preventing Spotlight from Indexing Time Machine Backups, External Disks and Network locations on a Mac:

1. Connect the volume you want excluded to the Mac, even if Spotlight is currently indexing.
2. Launch "**System Preferences**" and click on "**Spotlight**" followed by the "**Privacy**" tab.
3. Drag the drives icon into the "**Privacy**" window.

Disable .DS_Store File Creation

Mac OSX workstations create a file named .DS_Store which stores information about the custom attributes of its containing folder. These files are created automatically by Finder within any browsed directory. These files should be disabled from being created in order to maintain user performance while navigating a network directory structure. This change affects network drives using SMB/CIFS, AFP, NFS, and WebDAV.

1. Close all "**Finder**" Windows.
2. Open a "**Terminal**" session.
3. Execute the following command.

   ```
   defaults write com.apple.desktopservices DSDontWriteNetworkStores true.
   ```

4. Restart the workstation or log off and log in to the user account.

More information on .DS_Store can be found at https://support.apple.com/en-us/HT1629.

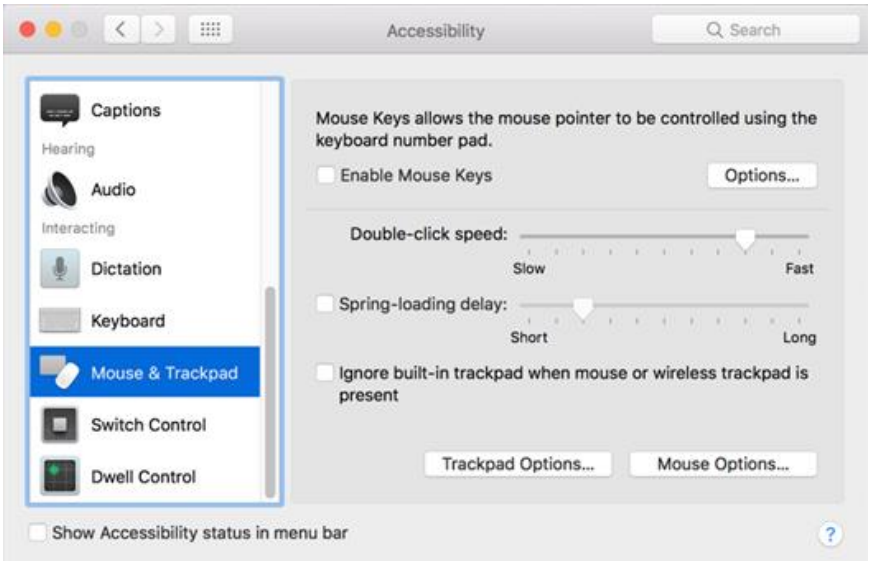
Disable Spring-Loaded Folders and Windows

Spring-loaded folders open folders in new windows while clicking-and-dragging items through a directory structure. This behavior can potentially cause unnecessary or unwanted caching of folder metadata as users traverse folders.

Max OSX 10.12

1. Open "**System Preferences**"
2. Navigate to "**Accessibility**"
3. Select "**Mouse & Trackpad**"
4. Uncheck the box "**Spring-loading delay**"

© 2020 NetApp, Inc. All Rights Reserved.



Mac OSX 10.5

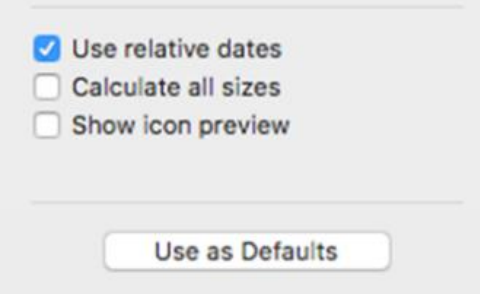
1. Open "**Finder**".
2. Open "**Finder Preferences'.**
3. Click the "**General" Tab.**
4. Uncheck the box "**Spring-loaded folders and windows**".

Disable Icon Previews

Some Icons in Finder can dynamically update based on the file's contents. If the content of the item is updated, then the item's icon will update to reflect those changes. This may cause the file to be cached locally at the branch office and may impact the user experience while navigating the virtual file share.

© 2020 NetApp, Inc. All Rights Reserved.

1. Open a “**Finder**” window.
2. Click the “**View**” menu.
3. Click “**Show View Options**”.
4. Uncheck the box to “**Show Icon Preview**”.
5. Click the button to “**Use as defaults**”.



© 2020 NetApp, Inc. All Rights Reserved.

12 End User Training

Please find below an example introduction email for end users, including training materials, do's and don'ts and overall best practices that apply when working on a centralized data set / collaborative environment. You can leverage this template and tailor to fit your organization's needs.

[CUSTOMER] recently invested in an enterprise IT solution that enables the organization to centralize all project data, local file servers with the objective to simplify data management and deliver real-time collaboration for all users in all offices.

GFC software helps [CUSTOMER] users to centralize their organization's data and simplify infrastructure management while delivering Global File Sharing with File Locking to the branch office workforce.

In summary, GFC creates a central 'Single Set of Data' in [CUSTOMER]'s data center while it's branch office GFC Intelligent File Caching mechanism transparently presents central file shares, documents and project files to the end user community in these branch offices. Additionally, GFC eliminates complexity, expensive storage and infrastructure at the branch while fully eliminating branch office backups.

In order to onboard the end user community, we have released a training video at https://youtu.be/RYvhnTz4bEA and for Architectural, Engineering and Construction customers at https://youtu.be/avMMA_ltZy0.

Accessing Project Folders and Files

[CUSTOMER] has created a unified namespace for the organization that is accessible to everyone by navigating to `\\corporate.local\public\`.

This network location can be accessed through a drive mapping i.e. I:\ or by navigating to the unified namespace using the network (UNC) path.

Cold Files Versus Warm Files

GFC only caches what's actively being used at the branch office locations, which means that some of the files within the central file set are cached and others are not.

- Cold file: the first time you open a file (marked with a grey X) the transfer of the file will take place over the Wide Area Network, which may take some time to complete
- Warm file: the second time you open the same file, the software will check if the cache maintains the latest version of the file, fetch any incremental updates from the central file server, and immediately serve the file to the end user

IMPORTANT: if you require access to a large-scale central project (i.e. > 500MB) that is not cached yet, it is recommended to schedule a pre-population job (overnight). You can request pre-population for a specific project folder by sending an email to support team at …@...

Do's and Don'ts

In a 'GFC' world there are specific do's and don'ts to adhere to in order to get the most out the solution and ensure everyone in the organization an optimal end user experience.

Do: Work directly of the FASTData File Share

- This file share will be presented to you by IT as a drive mapping (For example, I:\) or as a unified namespace using i.e. `\\corporate.local\public\`.
- You will recognize the file share by the "X" mark on some of the files (cold / uncached).

Don't: Copy data back and forth to your local computer / server

- Every file (when copied back) will be treated as a new file and therefore may impact bandwidth usage as minimum file differencing will take place at that moment.

© 2020 NetApp, Inc. All Rights Reserved.

- May cause inconsistencies in files, data loss as you might overwrite other user's files.
- Impacts the business and your own productivity.

Application-Specific Best Practices

There are specific applications that require additional attention from an end user perspective. Although [CUSTOMER] IT infrastructure teams have taken all measurements to automate the client-application best practices, some applications require additional settings to be configured or change in workflow.

Please consult the client application best practices documentation and training materials provided by your IT team.

For more information on GFC, please consult the following resources:

https://cloud.netapp.com/global-file-cache

13 Contact Details

Customer support for NetApp Global File Cache users with Cloud Volumes ONTAP, Cloud Volumes Services and Azure NetApp Files is available through these channels:

Product documentation, Case Management, Phone, Knowledgebase, Downloads, Tools, and more:
https://www.talonstorage.com/support

If you are an existing Talon Storage customer, please also use the link provided above for your support needs.

© 2020 NetApp, Inc. All Rights Reserved.

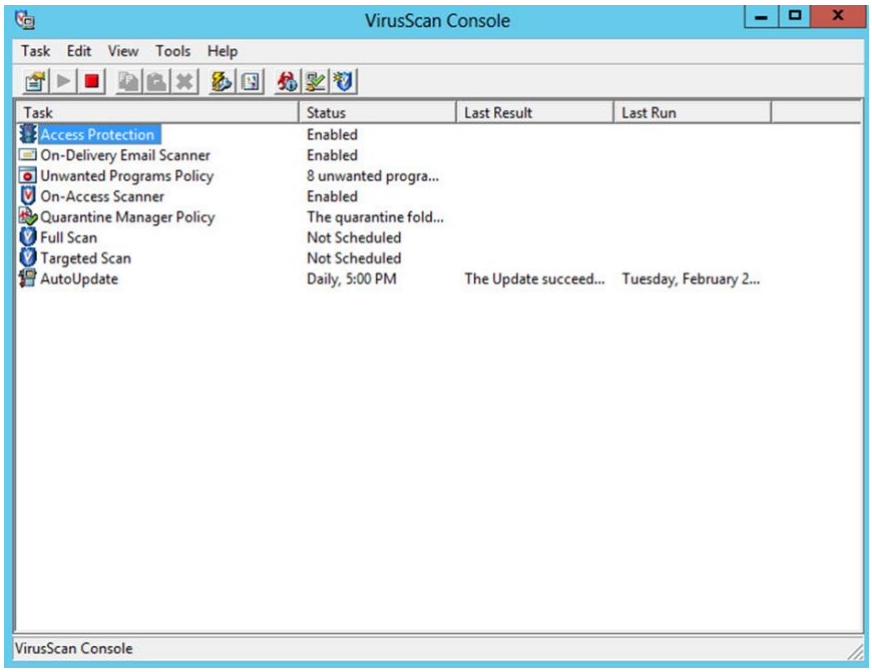
Appendix A: Antivirus Application Suites

McAfee VirusScan

Baseline Protection

After completing a Standard installation of the McAfee Virus Scan Enterprise and choosing to not perform the initial On-demand scan, follow the configuration specifics as outlined below, including On-Access Scanning, Full and Targeted Scan.

Figure 36)



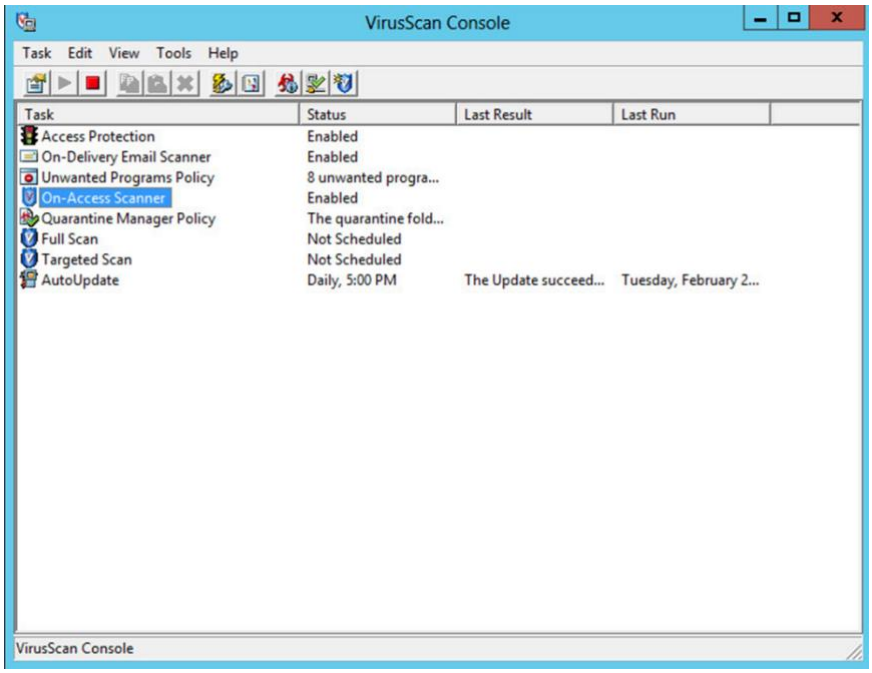
Excluding Services and Processes in McAfee VirusScan Console

This section details how to exclude NetApp Global File Cache (GFC) processes on Core/Edge Servers and other remote appliances based on McAfee VirusScan scanning.

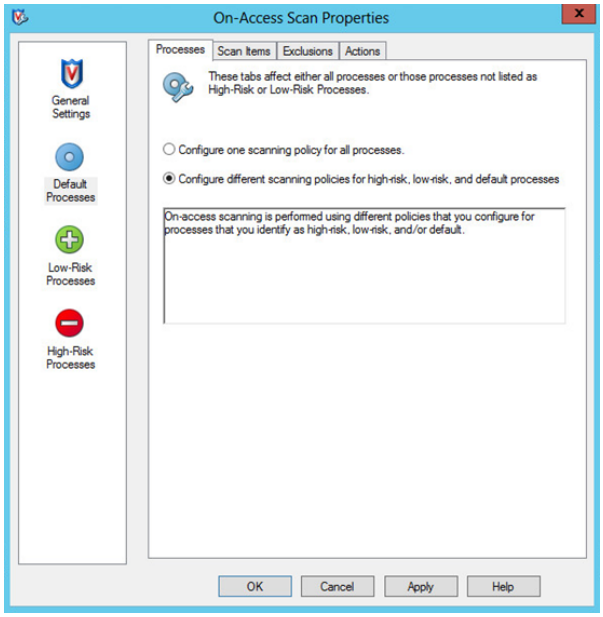
Note: Ensure that GFC processes, services, and drives are excluded on antivirus servers and clients and as a group policy for GFC users, if applicable.

1. Double click the "**On-Access Scanner**" task in the main VirusScan Console window.

© 2020 NetApp, Inc. All Rights Reserved.

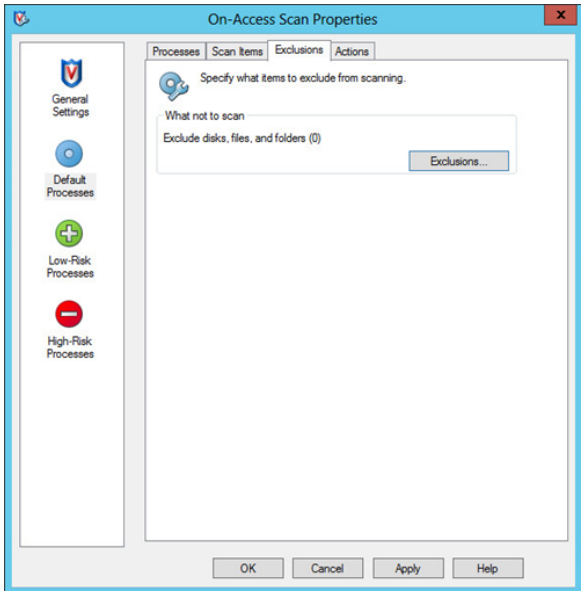


2. Click "**Default Processes**" in the left pane and then select the radio button labeled "**Configure different scanning policies for high-risk, low-risk, and default processes**"

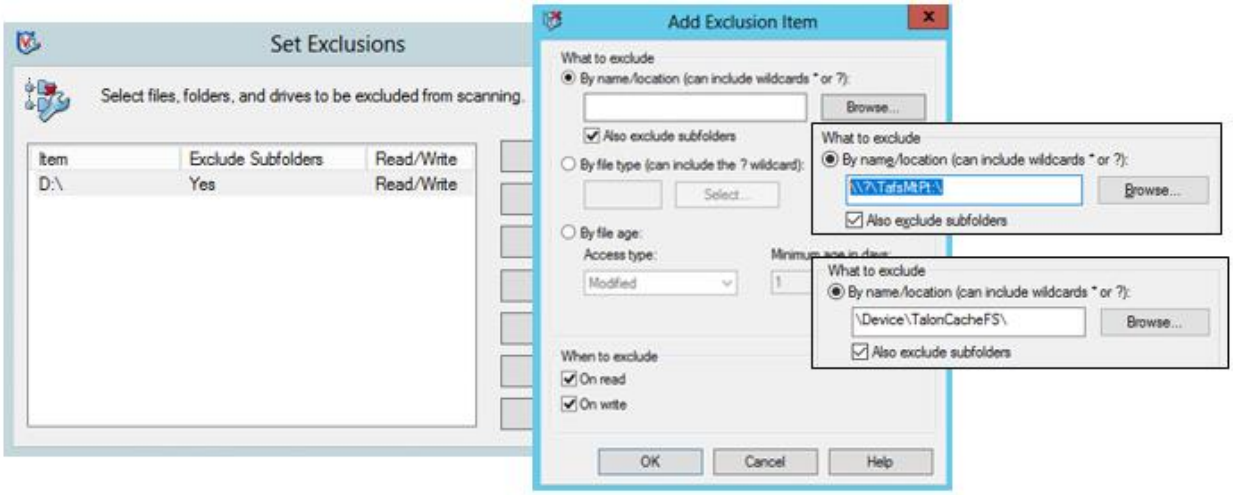


3. Click the "**Exclusions**" tab and then click the "**Exclusions…**" button to configure them

© 2020 NetApp, Inc. All Rights Reserved.

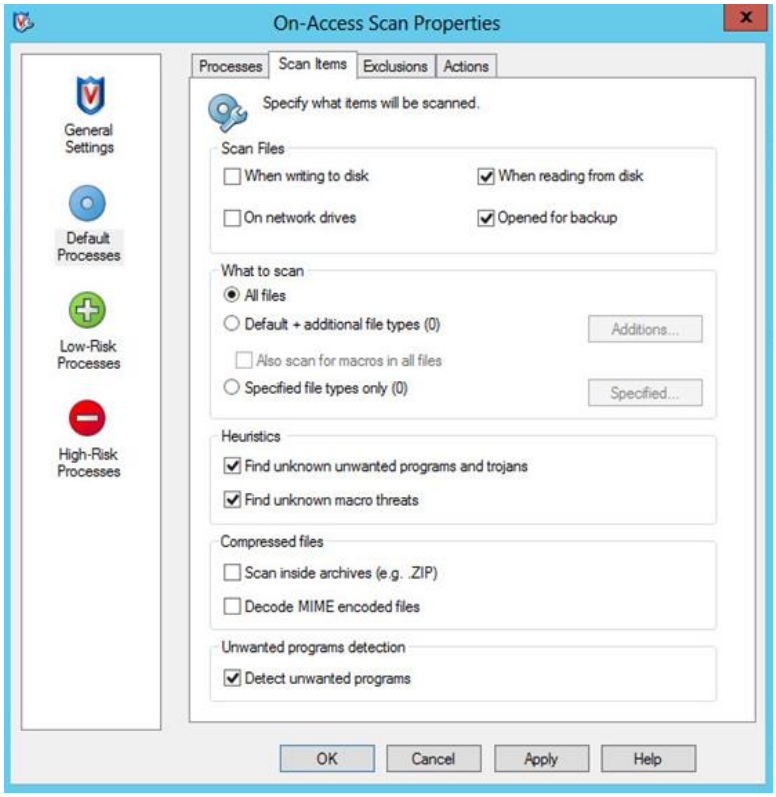


4. Add the D:\ drive to the Exclusions list. Additionally, add `\\?\TafsMtPt:\ or \\?\TafsMtPt*` and `\Device\TalonCacheFS\` to the Exclusions list. Ensure that subfolders are also excluded from scans. Click "**OK**" when finished

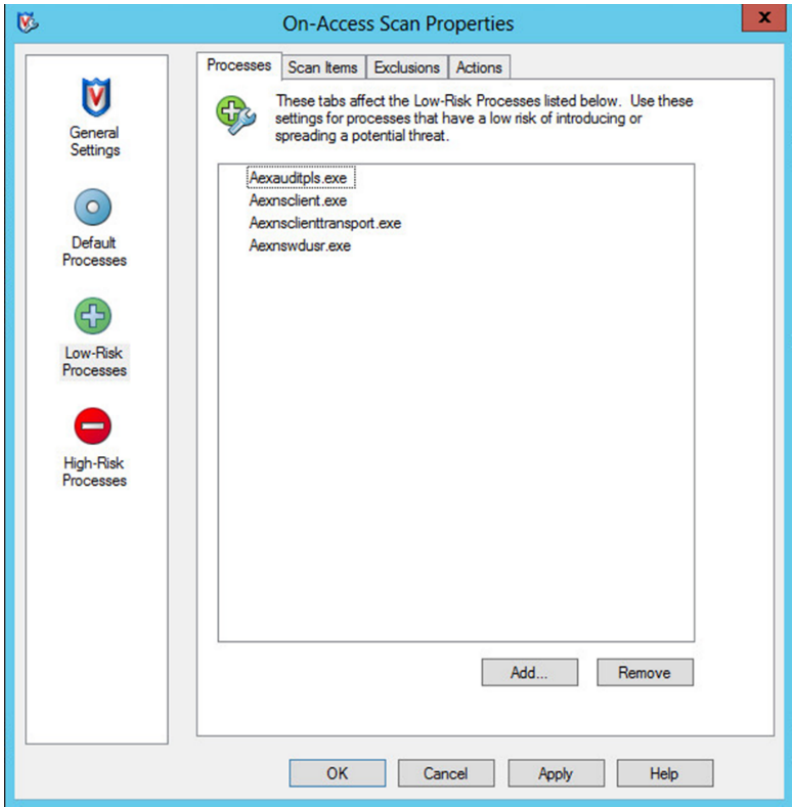


5. Click the "**Scan Items**" tab and de-select "**When writing to disk**"

© 2020 NetApp, Inc. All Rights Reserved.



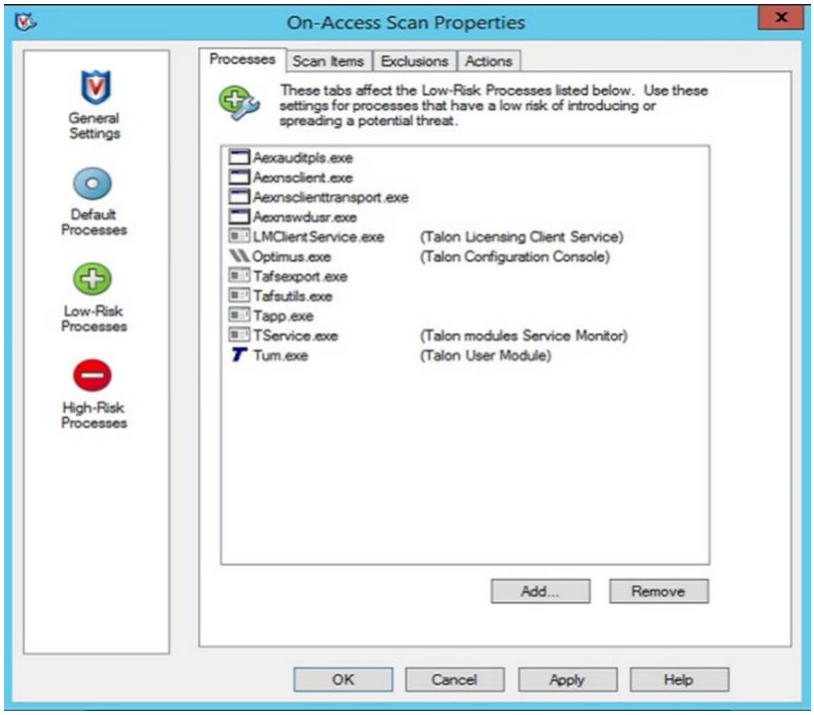
6. Click “**Low-Risk Processes**” in the left pane
7. Click the “**Add…**” button on the “**Processes**” tab



© 2020 NetApp, Inc. All Rights Reserved.

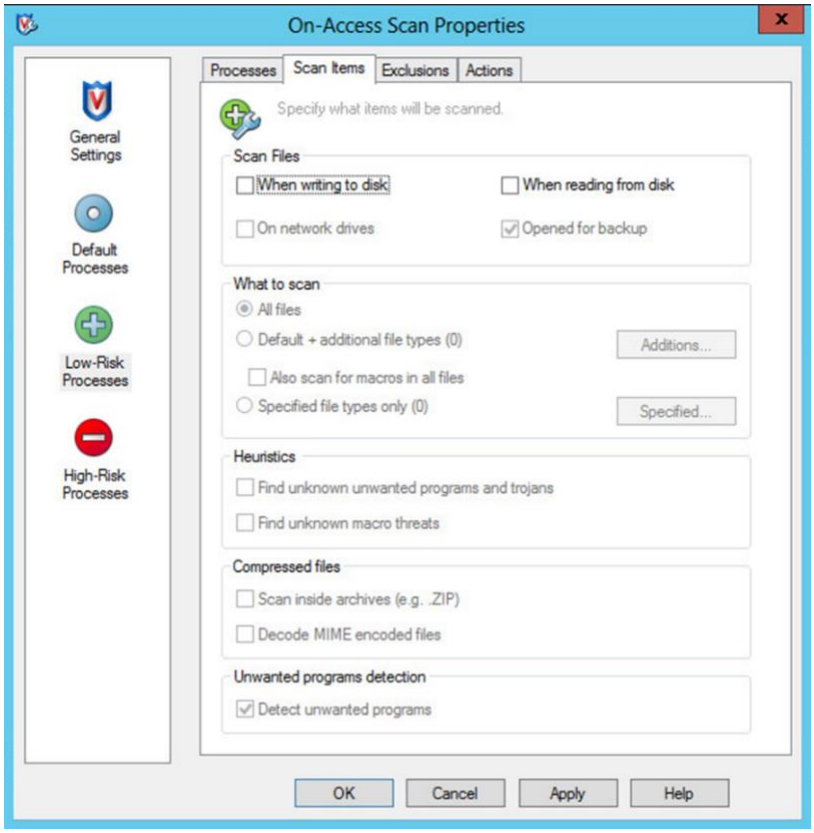
8. Once the list of available processes finishes populating, you may need to click the "**Browse…**" button and manually add the following processes:

```
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\tfs.exe
C:\Program Files\TalonFAST\Bin\TService.exe
C:\Program Files\TalonFAST\Bin\tum.exe
C:\Windows\System32\drivers\tfast.sys
C:\Program Files\TalonFAST\FastDebugLogs\
```

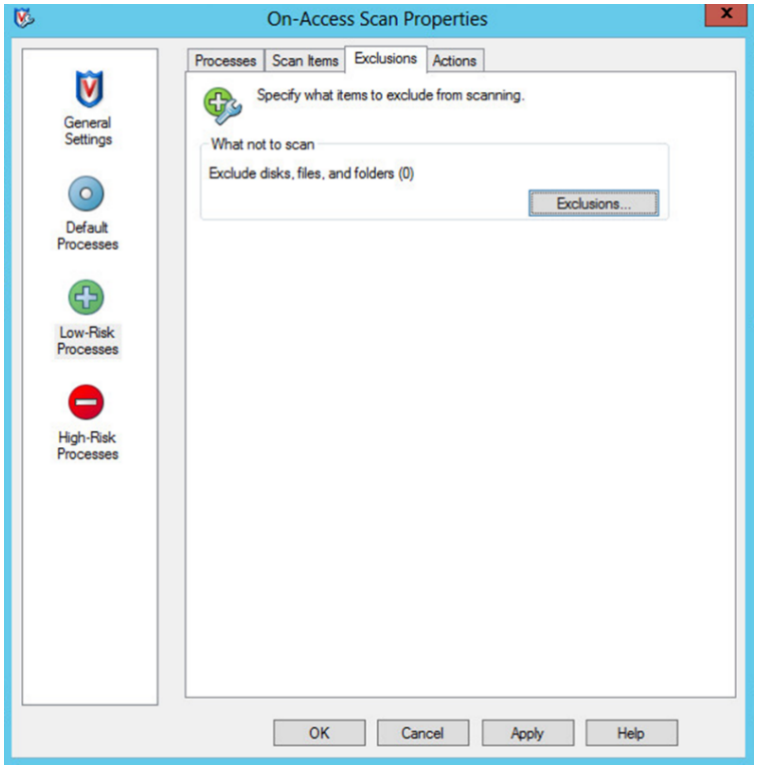


9. Click "**OK**" to apply the changes
10. Click the "**Scan Items**" tab and de-select "**When writing to disk"** and "**When reading from disk**"

© 2020 NetApp, Inc. All Rights Reserved.



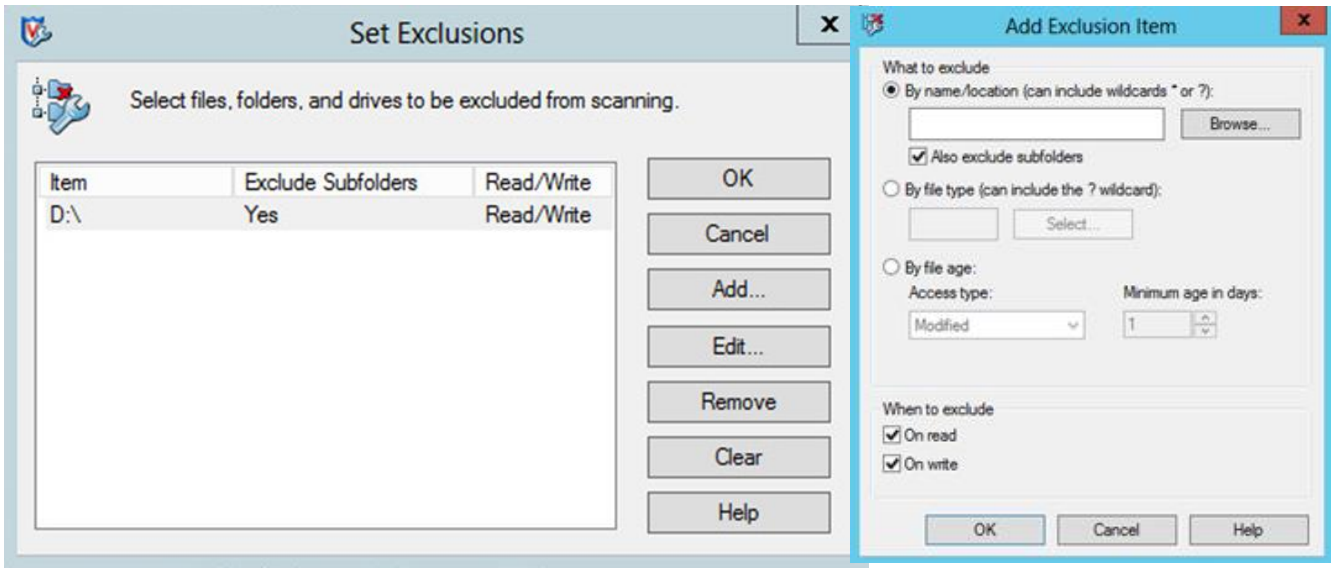
11. Click the “**Exclusions**” tab at the top
12. Click the “**Exclusions…**” button

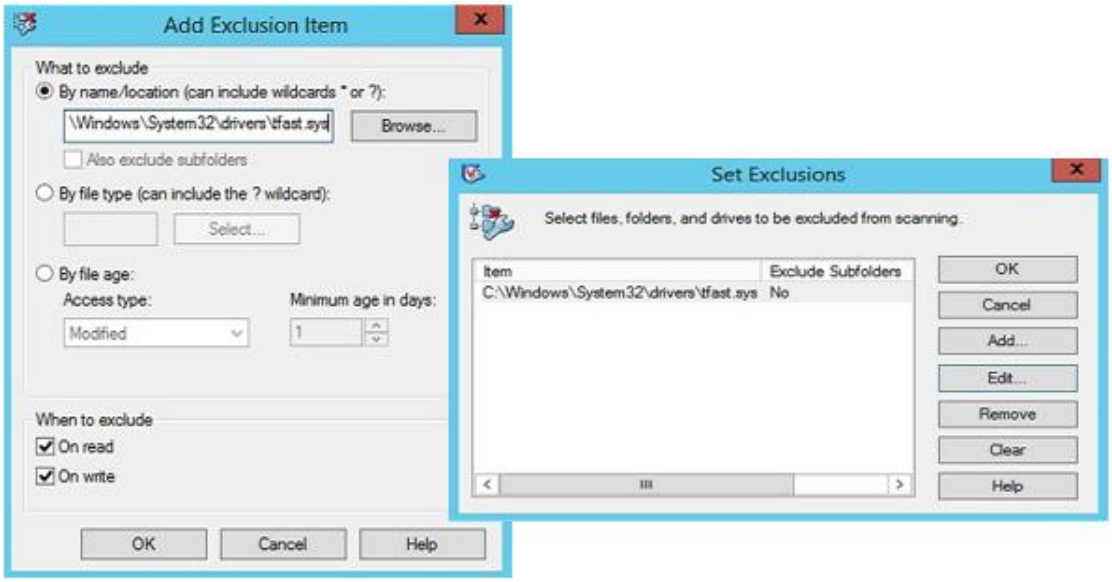


© 2020 NetApp, Inc. All Rights Reserved.

13. Add the D:\ drive to the Exclusions list. Additionally, add `\\?\TafsMtPt:\` and `\Device\TalonCacheFS\` to the Exclusions list. Ensure that subfolders are also excluded from scans. Click “OK” when finished
14. Add `C:\Windows\System32\drivers\tfast.sys`

    Note: You may have to manually type in this path to add tfast.sys
15. Click “**OK**” when finished.



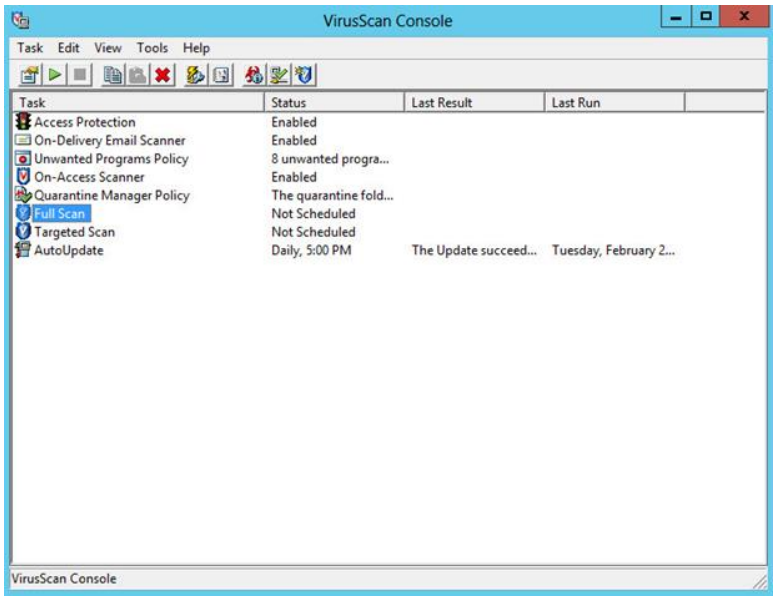


Full or Targeted Scans

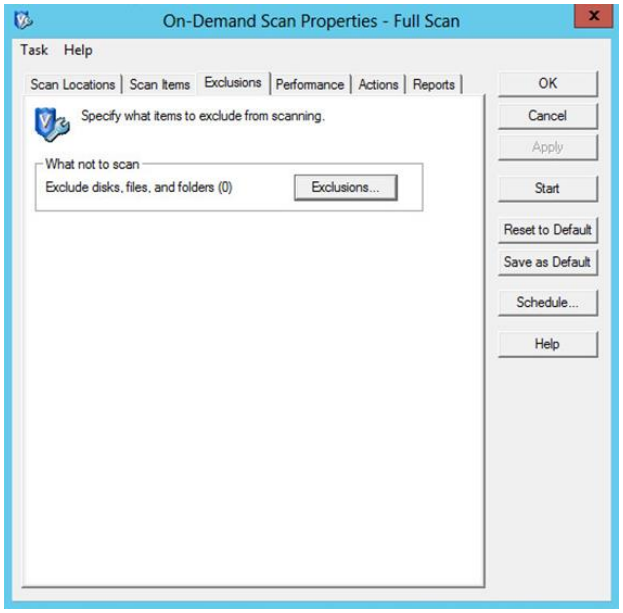
If running a full or targeted scan on a GFC server, please follow the steps below

1. Double click either “**Full Scan**” or “**Targeted Scan**” from the VirusScan Console

© 2020 NetApp, Inc. All Rights Reserved.

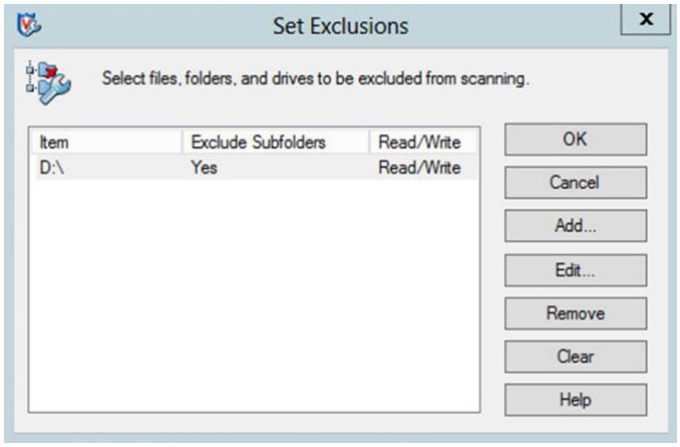


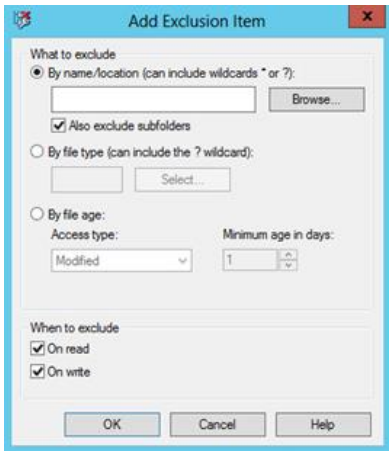
2. Click the “**Exclusions**” tab from the On-Demand Scan Properties window. Click the “**Exclusions…**” button.



3. Add the D:\ drive to the Exclusions list. Additionally, add `\\?\TafsMtPt:\` and `\Device\TalonCacheFS\` to the Exclusions list. Ensure that subfolders are also excluded from scans. Click “**OK**” when finished

© 2020 NetApp, Inc. All Rights Reserved.



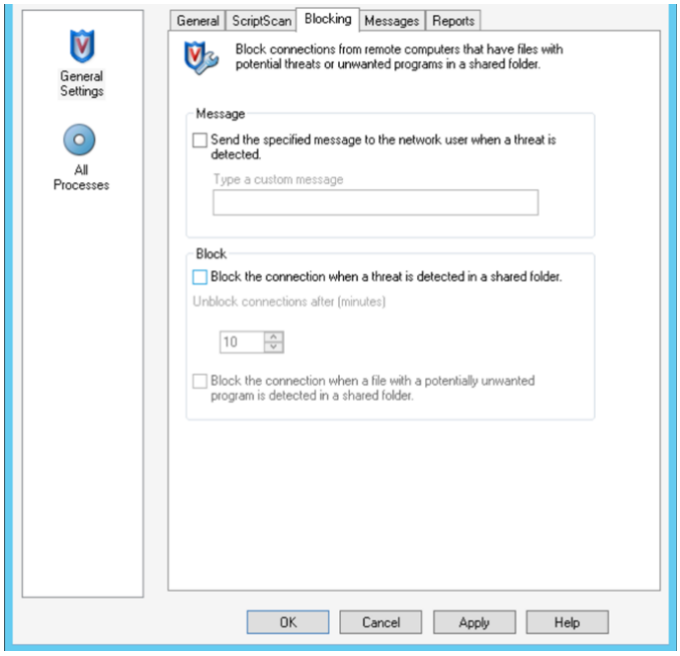


Prevent Connection Blocking in Shared Folders

With the exclusions of the D:\ drive, it is recommended that connections not be blocked from shared folders. This will provide consistent file access from the GFC Virtual File Share.

To disable the connection blocking, uncheck the box as shown below:

Figure 37)

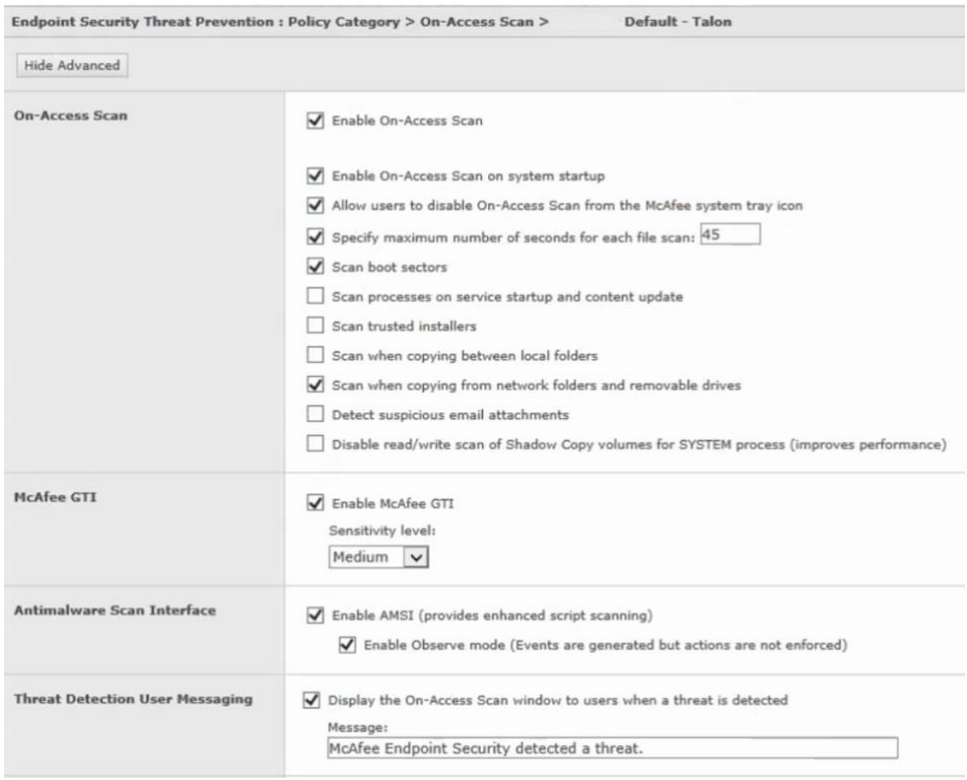


McAfee VirusScan - Central Management Console

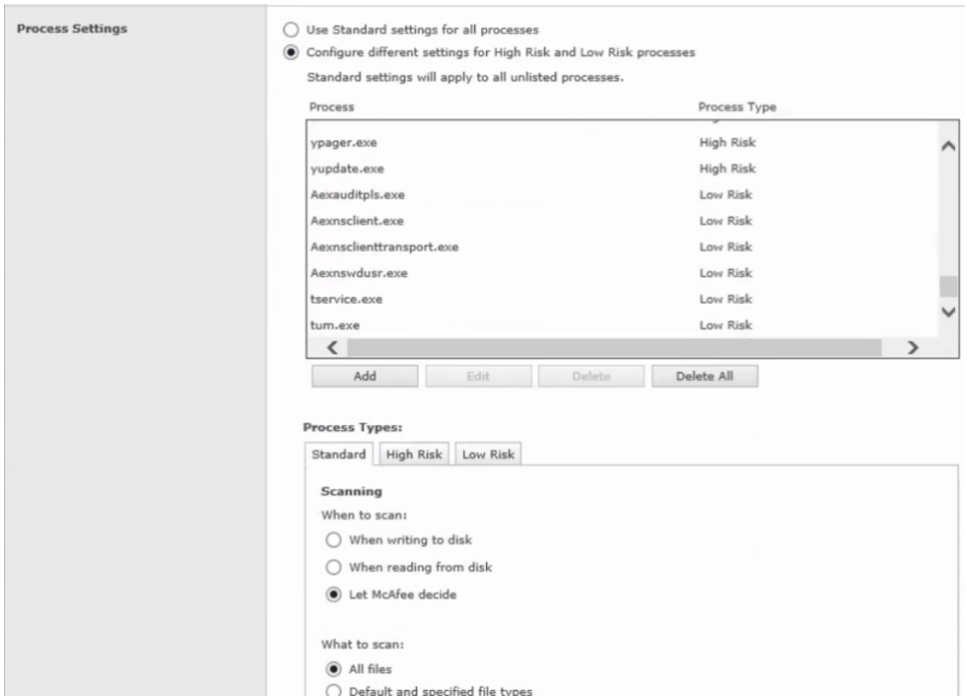
Go to the McAfee centralized management console and create a new Threat Prevention policy for the GFC servers and associate the GFC Core and Edge servers with the policy.

1. Open the GFC Policy and click on "**Show Advanced settings**"
2. Ensure the settings have been configured as below

© 2020 NetApp, Inc. All Rights Reserved.



3. The process settings need to be configured for High Risk and Low Risk
   a. Ensure the tservice.exe and tum.exe are configured as "**Low Risk**"

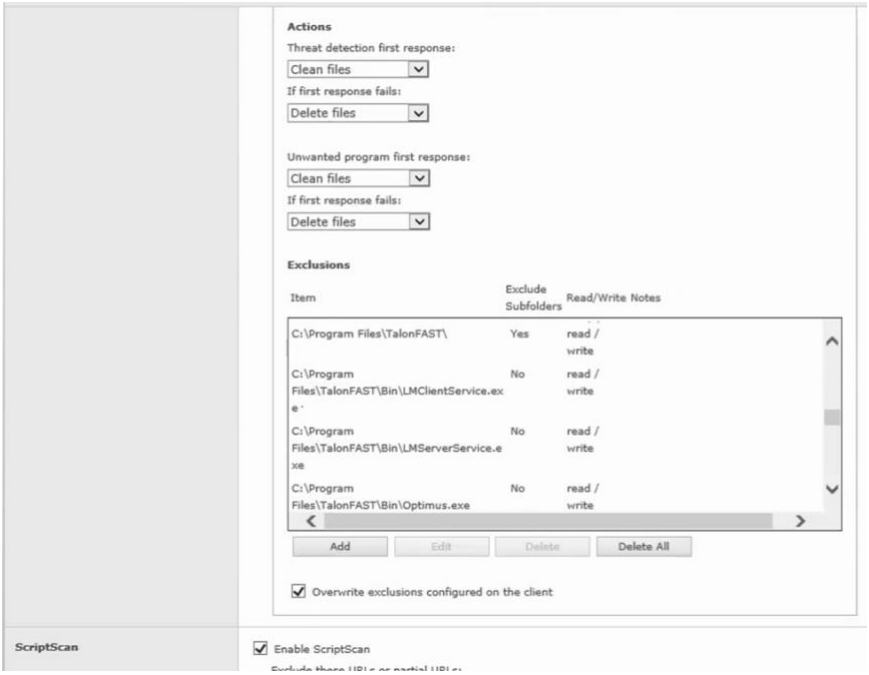


4. The exclusion includes the following exclusions:

`D:\`

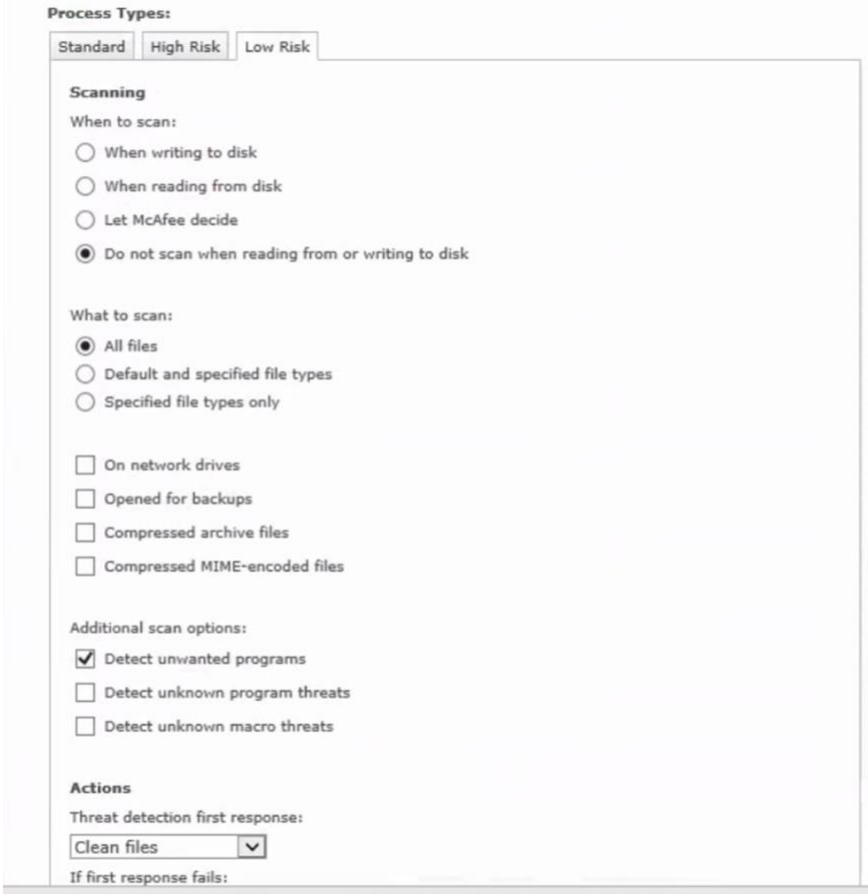
© 2020 NetApp, Inc. All Rights Reserved.

```
D:\LocalFASTData\
C:\Program Files\TalonFAST\FastDebugLogs\
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\tfs.exe
C:\Program Files\TalonFAST\Bin\TService.exe
C:\Program Files\TalonFAST\Bin\tum.exe
C:\Windows\System32\drivers\tfast.sys
\Device\TalonCacheFS\
\\?\TafsMtPt:\ or \\?\TafsMtPt* (Depends on the current version)
*TAFS
Policydb.xml
```



5. Under the low risk configuration for Process Type ensure scanning is set to the following
   a. “Do not scan when reading from or writing to disk”.

© 2020 NetApp, Inc. All Rights Reserved.



Symantec Endpoint Protection 12.x

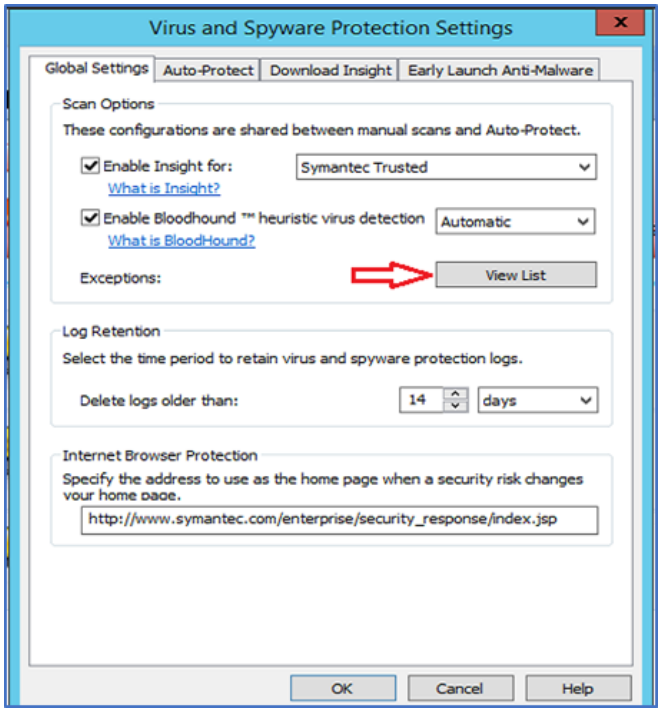
This section outlines best practices for Symantec Endpoint Protection version 12.x targeted for GFC appliances based on Windows Server.

1. Double click the Symantec icon on the task bar

2. "**Virus and Spyware Protection**" -> Click "**Options" -> "Change Settings**"

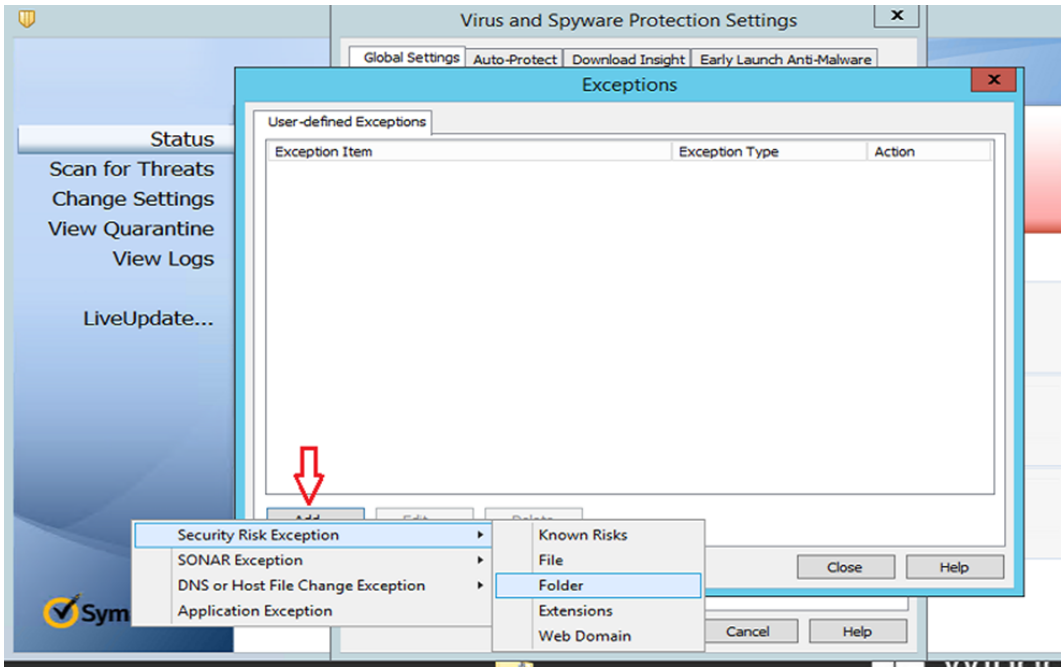
© 2020 NetApp, Inc. All Rights Reserved.

3. Click “**View List**”

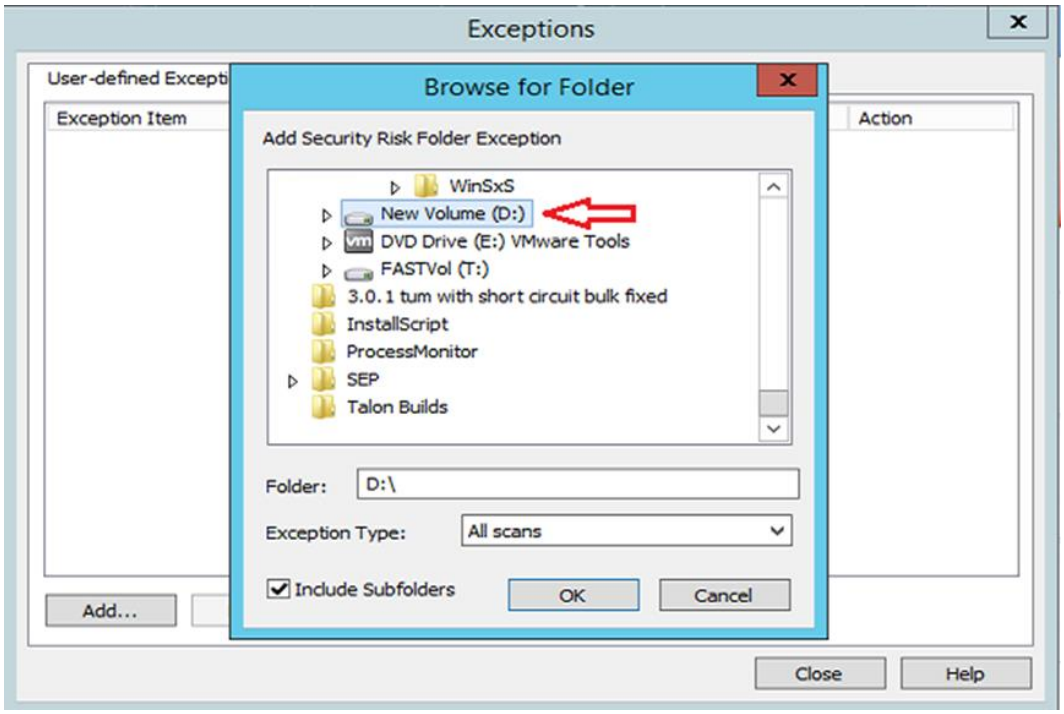


4. Click “**Add**” -> “**Security Rick Exception**” **-> “Folder**”

© 2020 NetApp, Inc. All Rights Reserved.

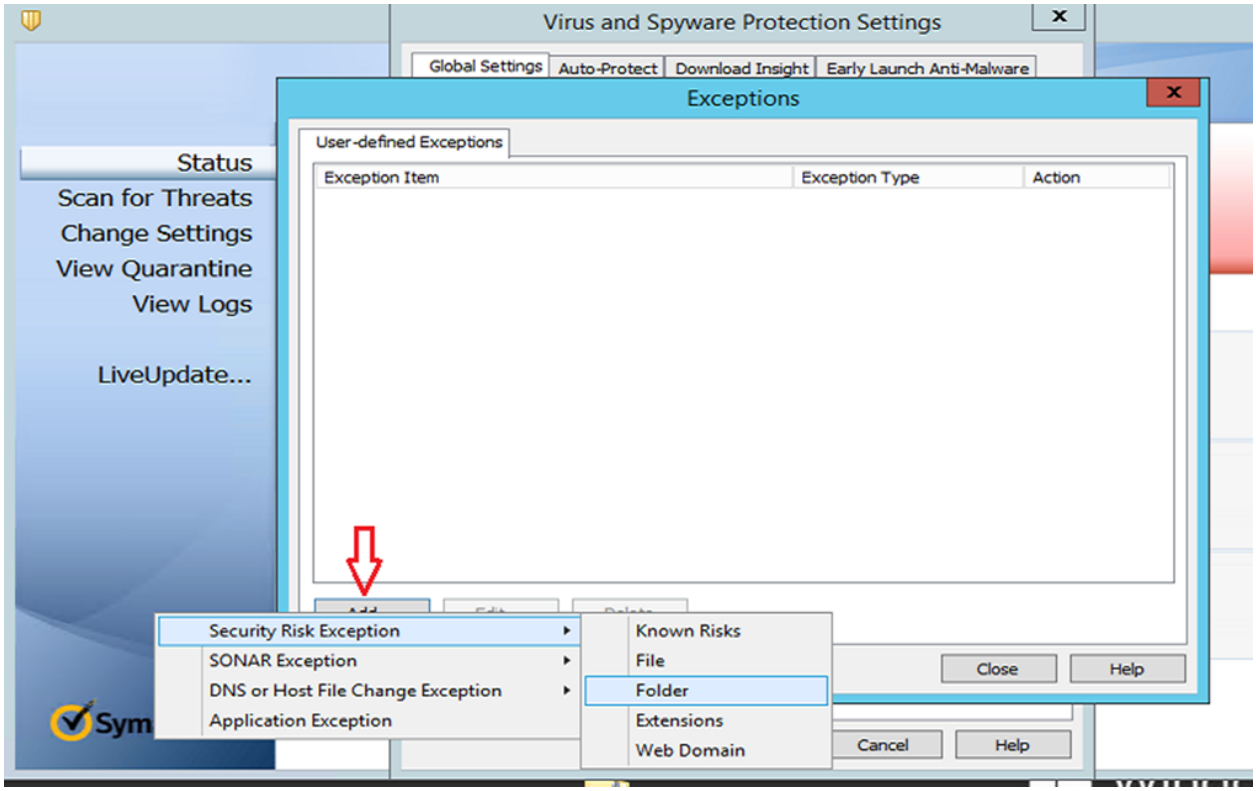


5. Scroll down, click on D:\, and click "**OK**"



6. Click "**Add**" -> "**Security Risk Exception**" -> "**Folder**"

© 2020 NetApp, Inc. All Rights Reserved.

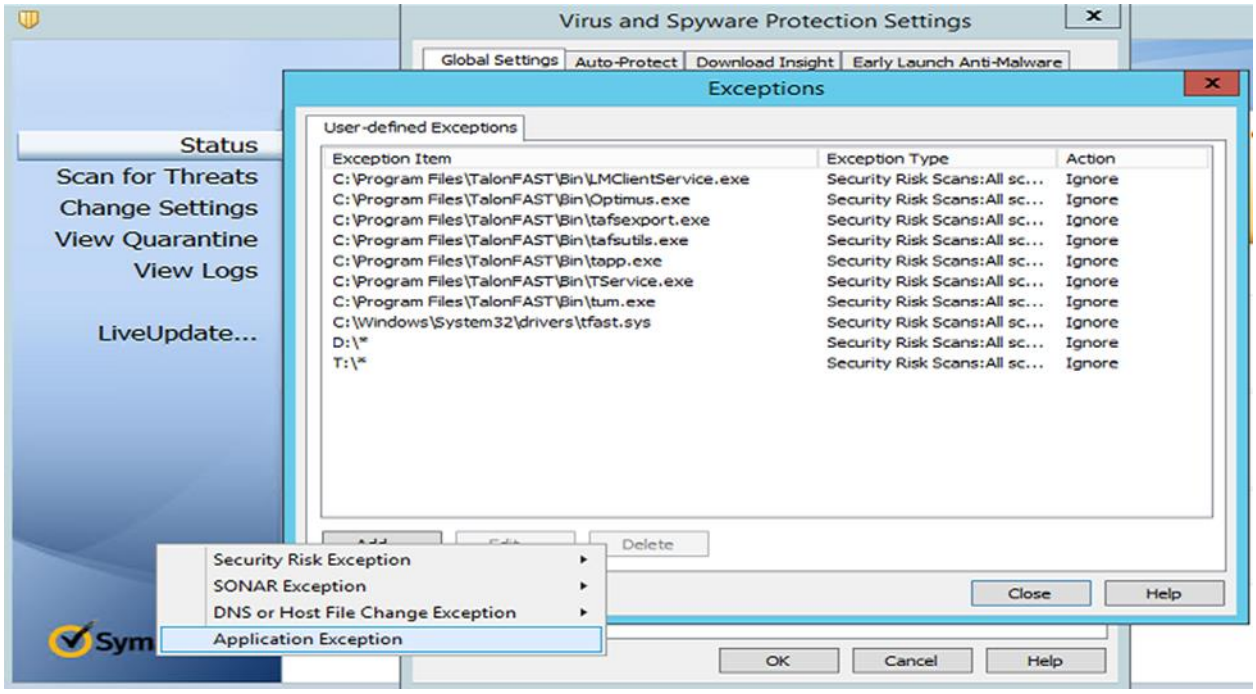


7. Add the following:

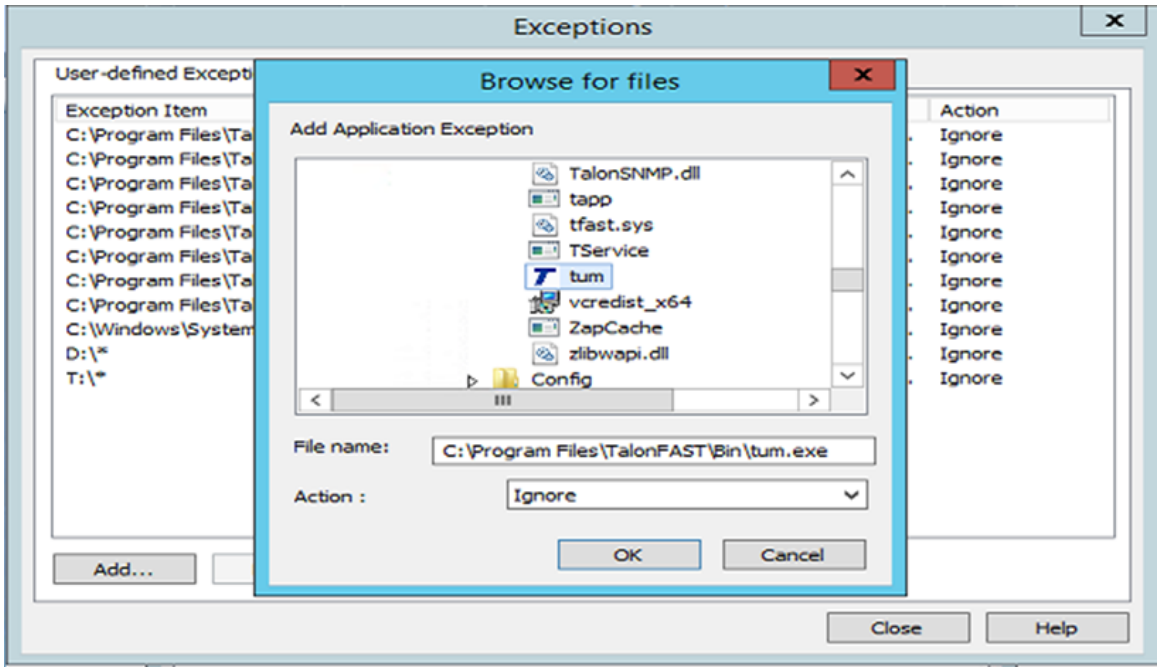
```
C:\Program Files\TalonFAST\Bin\LMClientService.exe
C:\Program Files\TalonFAST\Bin\LMServerService.exe
C:\Program Files\TalonFAST\Bin\Optimus.exe
C:\Program Files\TalonFAST\Bin\tafsexport.exe
C:\Program Files\TalonFAST\Bin\tafsutils.exe
C:\Program Files\TalonFAST\Bin\tapp.exe
C:\Program Files\TalonFAST\Bin\tfs.exe
C:\Program Files\TalonFAST\Bin\TService.exe
C:\Program Files\TalonFAST\Bin\tum.exe
C:\Windows\System32\drivers\tfast.sys
\\?\TafsMtPt:\ or \\?\TafsMtPt*
\Device\TalonCacheFS\
```

8. **Click “Add” ->** “Application Exception”

© 2020 NetApp, Inc. All Rights Reserved.

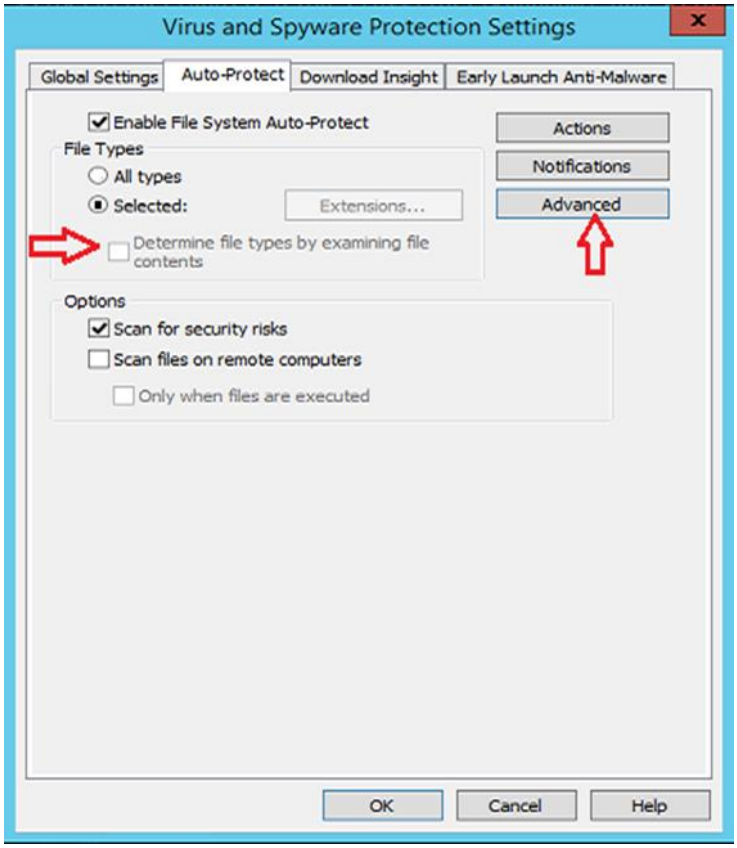


9. Browse to `C:\Program Files\TalonFAST\Bin\` and add `tum.exe`

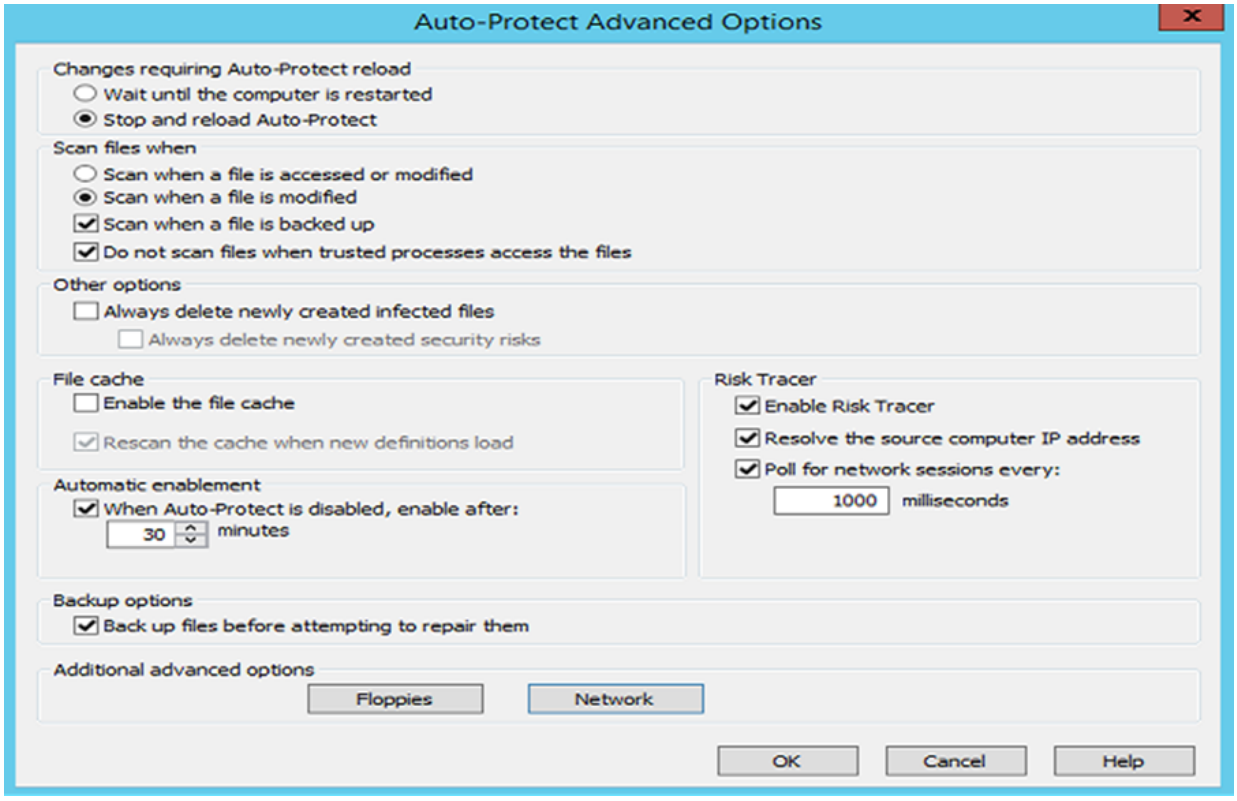


10. Click "**OK**"
11. Click on the "**Auto-Protect**" tab. Under "**File Types**," click "**Selected**." Uncheck "**Determine file types by examining file contents**." Click "**Advanced**."

© 2020 NetApp, Inc. All Rights Reserved.

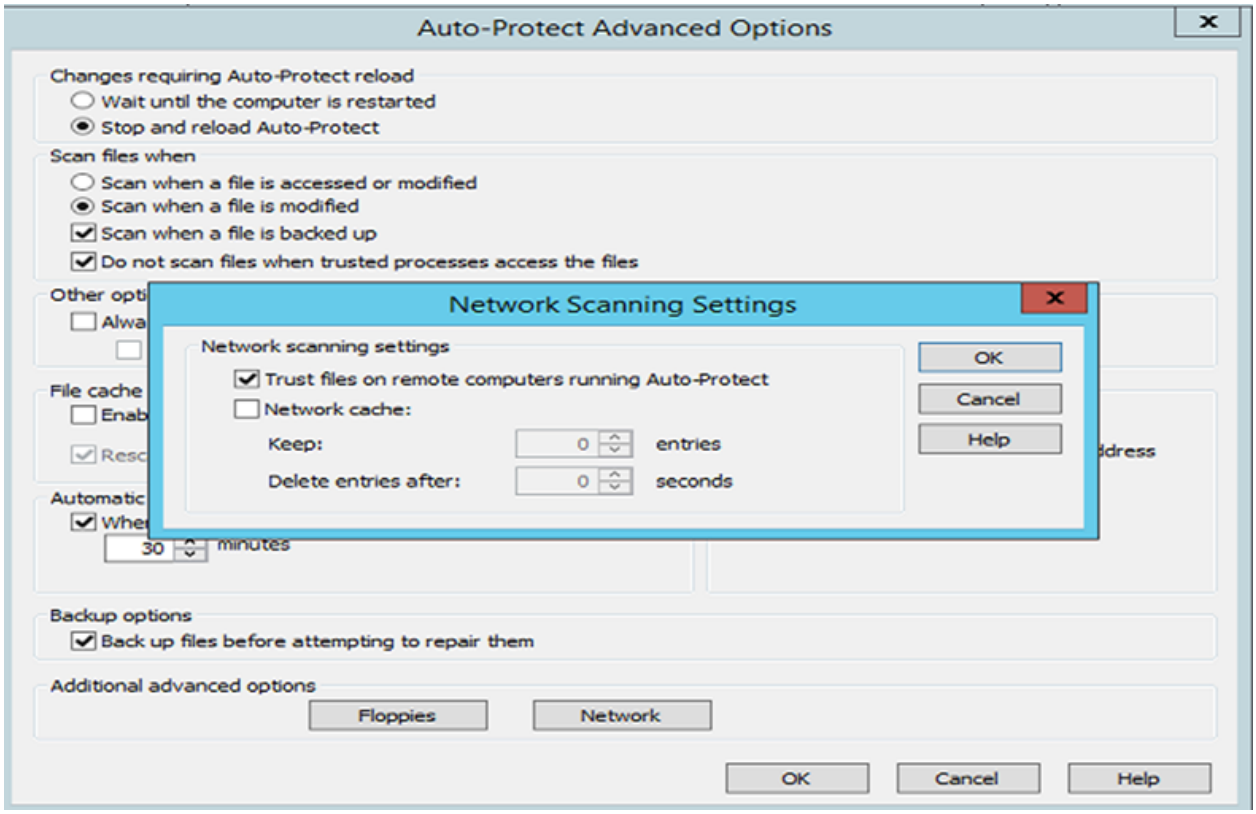


12. Adjust settings as shown below

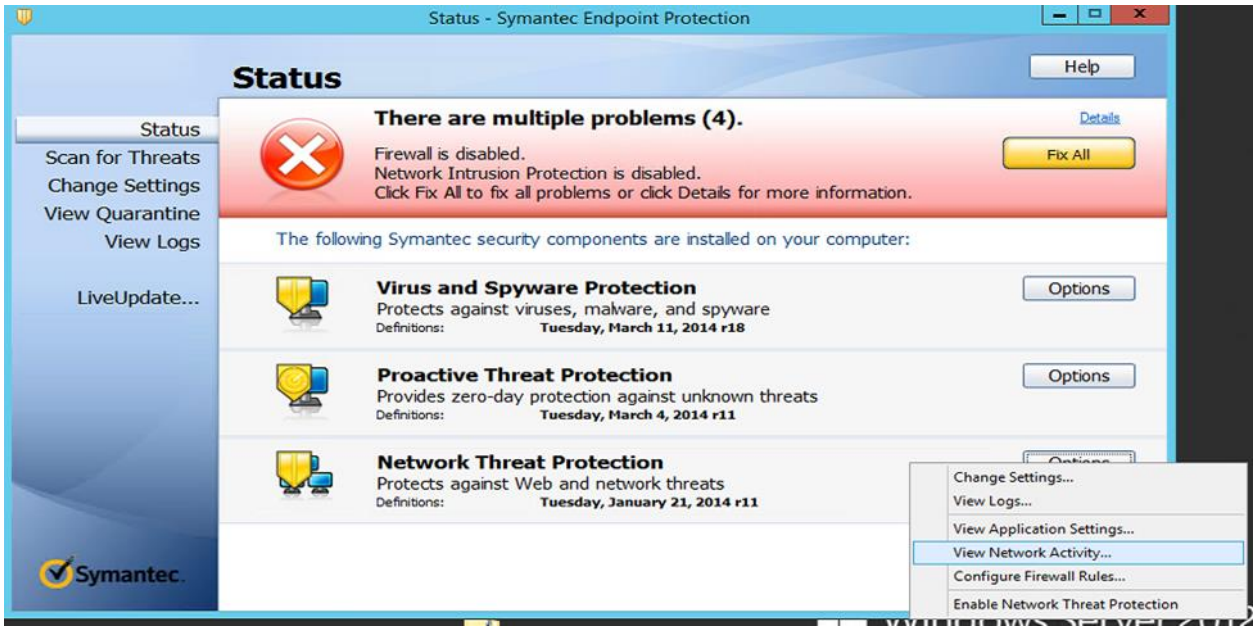


© 2020 NetApp, Inc. All Rights Reserved.

13. Click “**Network**”
14. Uncheck “**Network cache**”

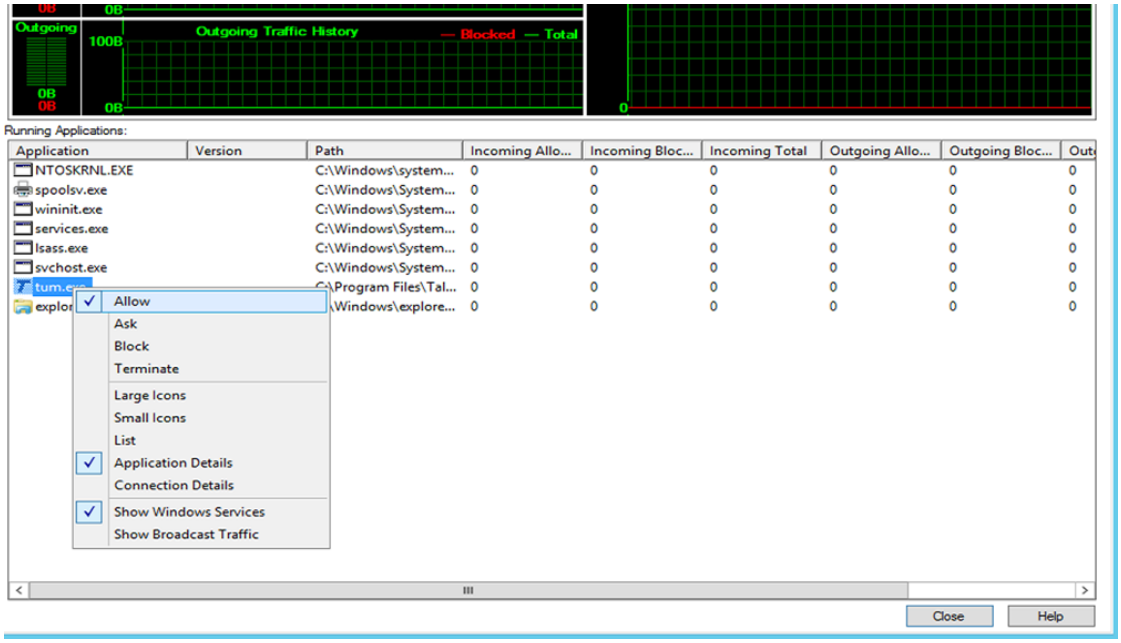


15. Click “**OK**”
16. “**Network Threat Protection**” -> Click “**Options**” and select “**View Network Activity**”



17. Right click `tum.exe` and select “**Allow**”

© 2020 NetApp, Inc. All Rights Reserved.



Configuration is complete.

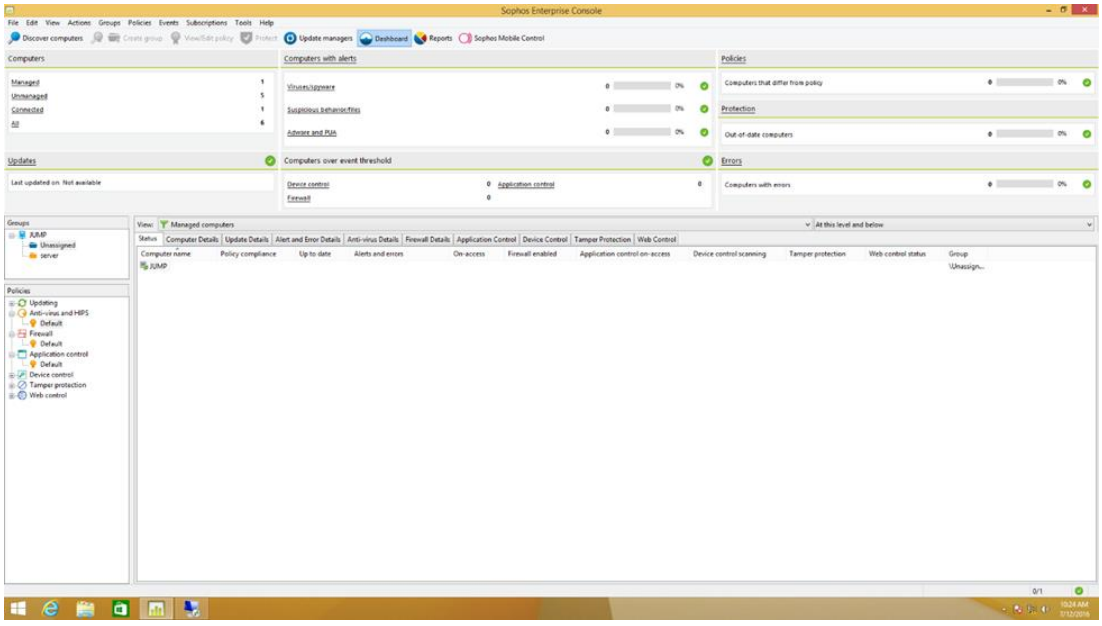
Sophos Endpoint Security and Control v10.x

This section outlines best practices for Sophos Endpoint Security and Control targeted for GFC appliances based on Windows Server.

Baseline Protection (Enterprise Console Configuration)

After completing a typical installation of the Sophos Enterprise Console, follow the configuration specifics as documented below. This process outlines the procedure to configure Sophos Endpoint Security and Control from a central configuration perspective.

Figure 38)



© 2020 NetApp, Inc. All Rights Reserved.

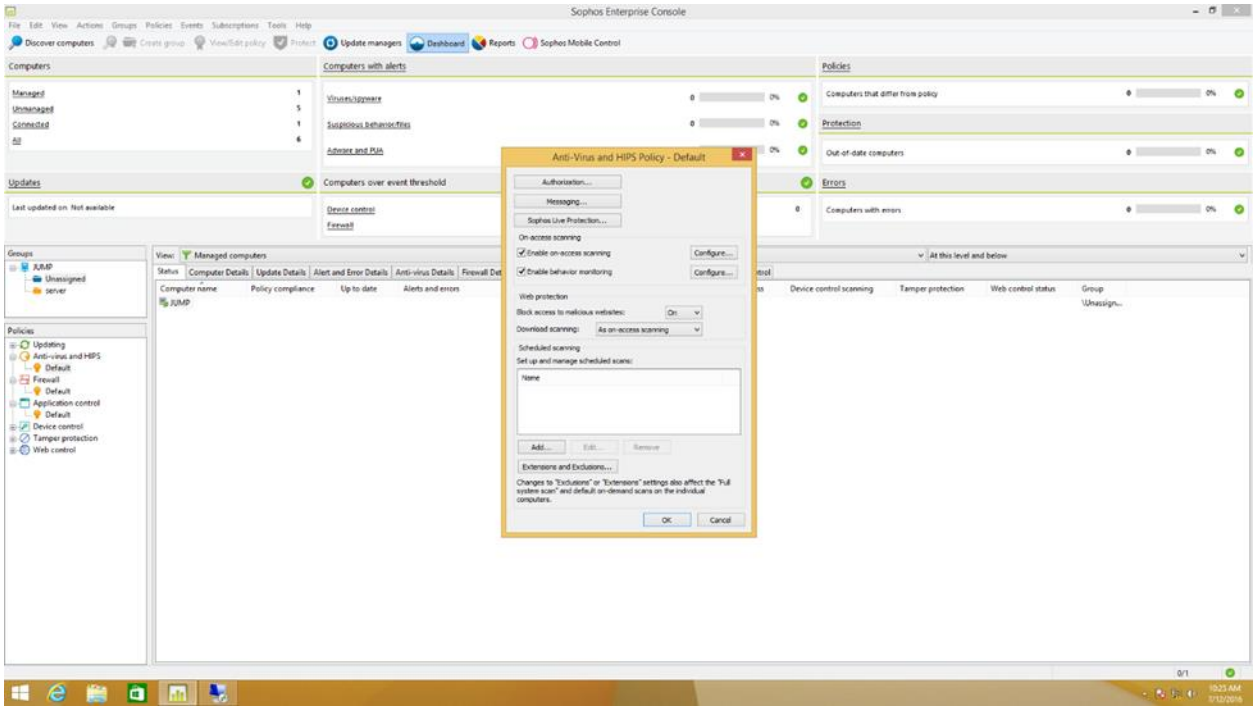
Excluding Services and Processes using Sophos Enterprise Control

This section details how to exclude GFC processes on server and remote appliances from Sophos antivirus scanning.

Note: Ensure that GFC processes, services, and drives are excluded from antivirus scanning

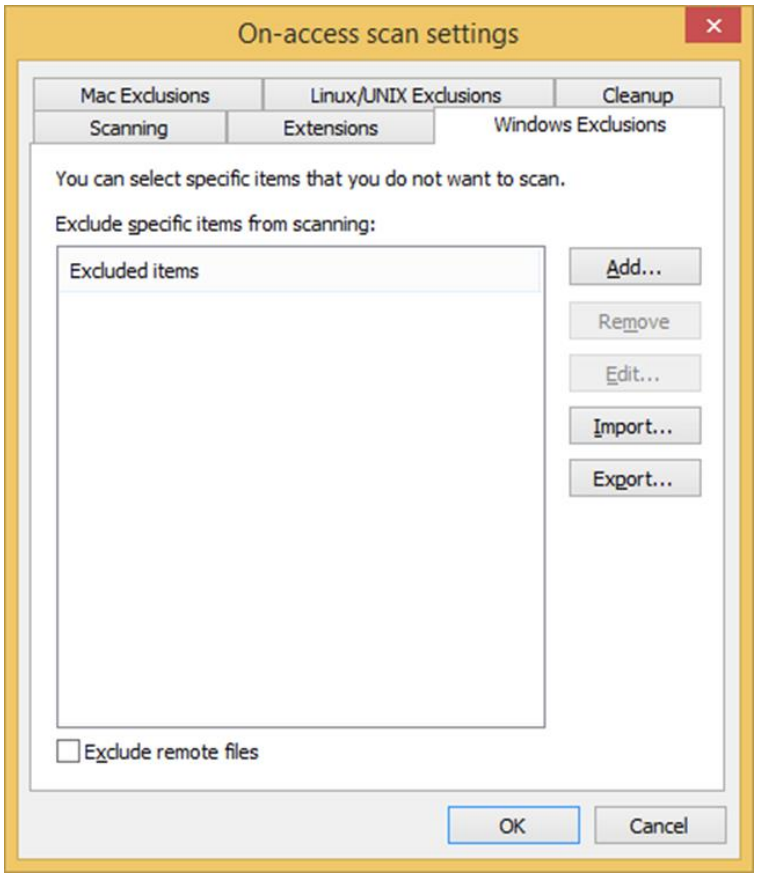
These changes should be made to Server and Client policies as well as group policy for GFC users if applicable:

1. Expand the "**Anti-Virus and HIPS**" tree in the "**Policies**" section of the Enterprise Console. Double-click the policy you wish to adjust.



2. Click the "**Configure…**" button next to Enable on-access scanning
3. Click the "**Windows Exclusions**" tab

© 2020 NetApp, Inc. All Rights Reserved.



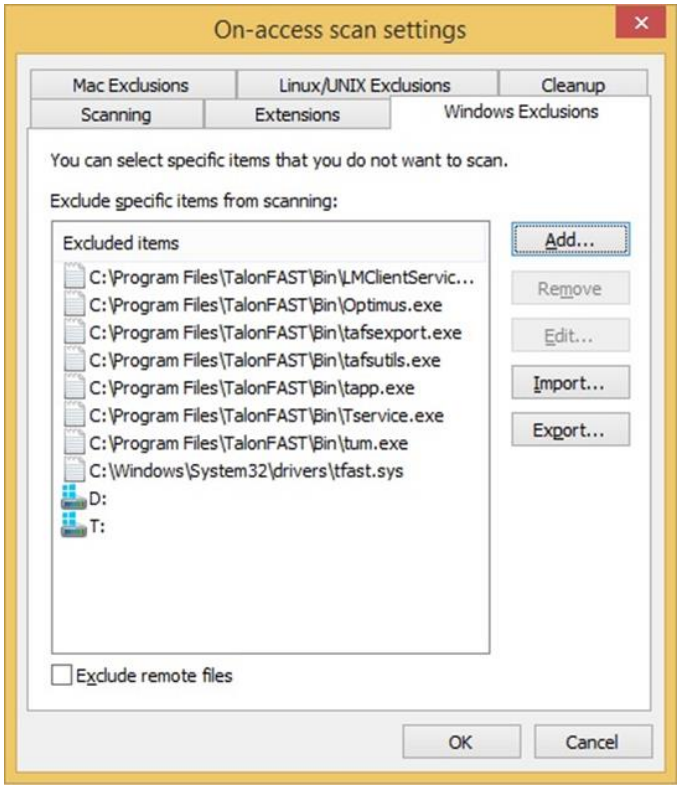
4. Add the following items to the Excluded Items list and click OK when finished:

```
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\tfs.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
D:\
\\?\TafsMtPt:\ or \\?\TafsMtPt*
\\?\GLOBALROOT\Device\TalonCacheFS\
\\?\GLOBALROOT\Device\TalonCacheFS\*
\Device\TalonCacheFS\
```

Exclude `Process tum.exe`

Exclude `Process tapp.exe`

© 2020 NetApp, Inc. All Rights Reserved.

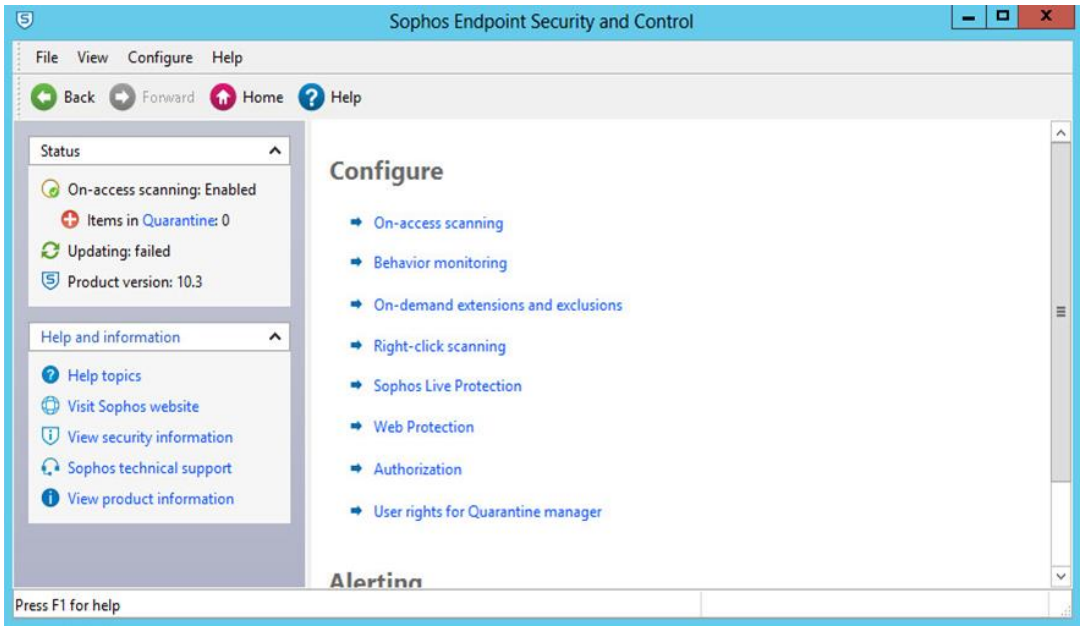


To verify the central configuration results on a connected client machine, we can use the Sophos Endpoint Security and Control panel.

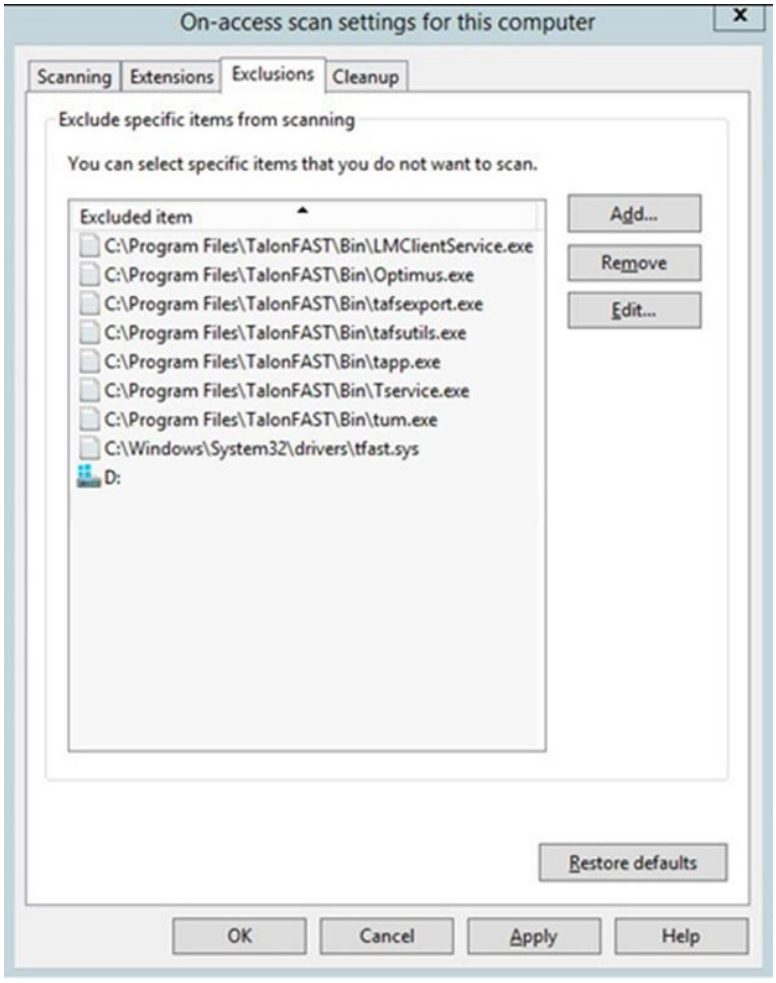
5. Click "**Configure anti-virus and HIPS**".

6. Click "**On-access scanning**"

© 2020 NetApp, Inc. All Rights Reserved.



7. Click the "**Exclusions**" tab to verify that the correct policy and exclusions have been applied to the appliance



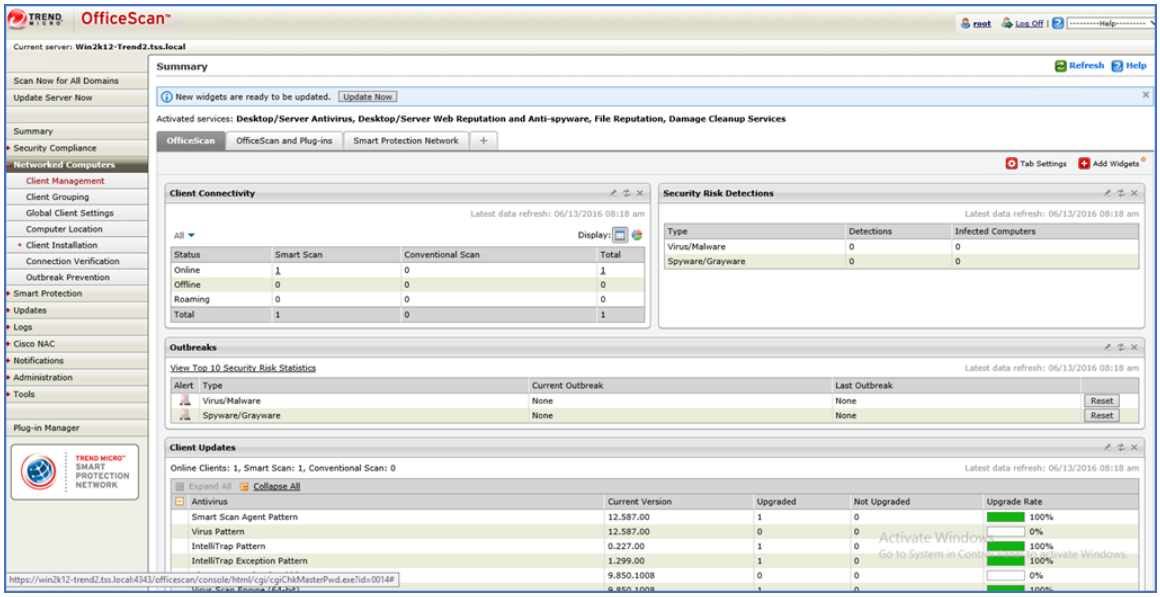
© 2020 NetApp, Inc. All Rights Reserved.

Sophos built in Firewall

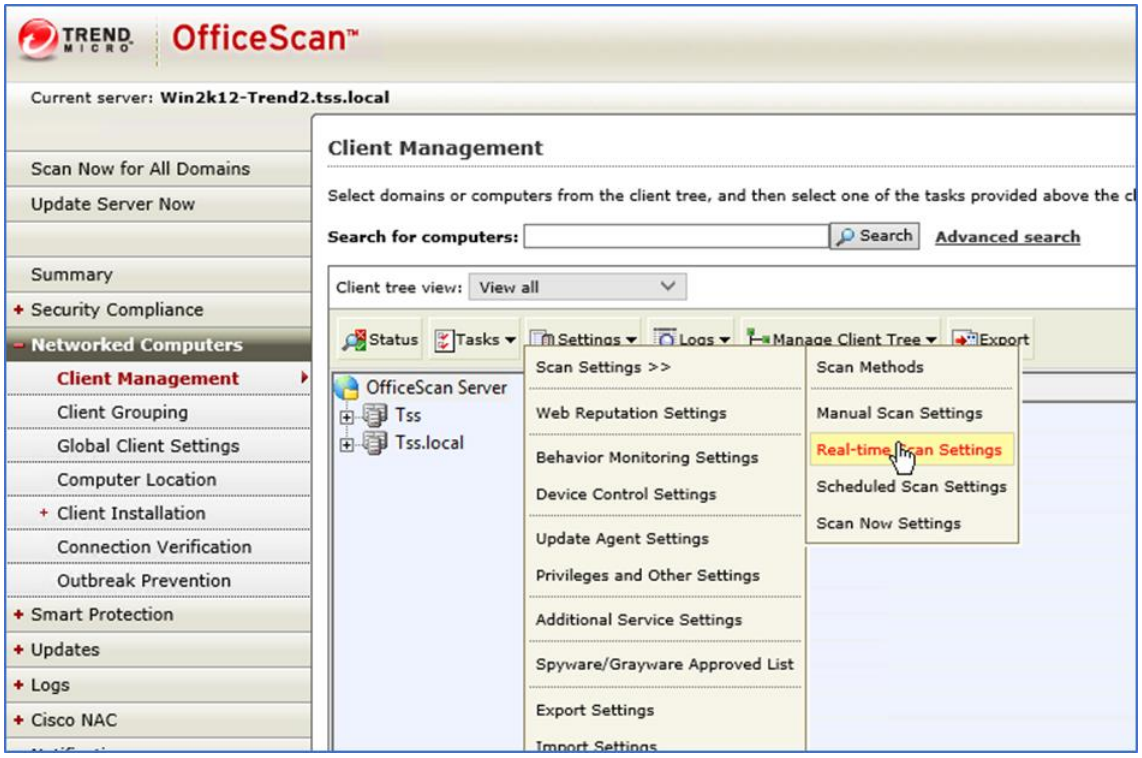
Microsoft Windows Server 2016 and 2019 by default includes a Microsoft Windows Firewall. GFC automatically provides a script to perform Microsoft Windows firewall maintenance, allowing ports associated with GFC. GFC recommends the use of the Microsoft Windows firewall.

Trend Micro Officescan

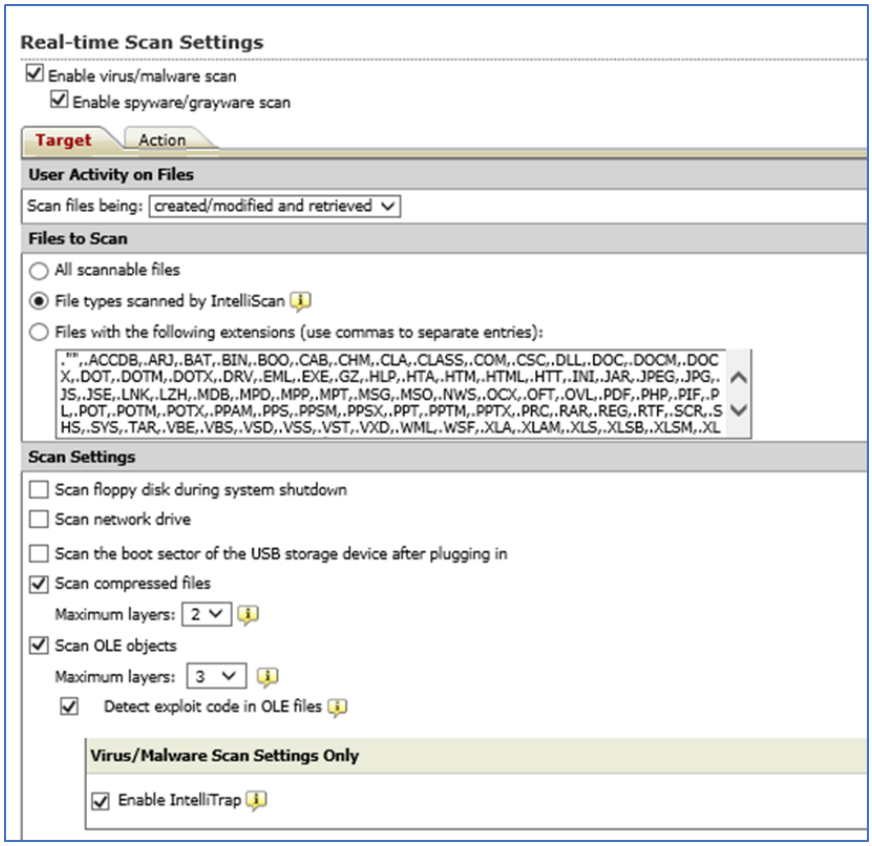
1. Open the Management GUI and navigate to “**Networked Computers**” -> “**Client Management**”.



2. Navigate to “**Scan Settings**”-> ”**Real-Time Scan Settings**”



© 2020 NetApp, Inc. All Rights Reserved.



3. On the "**Target**" tab, enable "**File types scanned by IntelliScan**".
4. Directory scanning. Scroll down and add the following exclusions to "**Scan Exclusion List (Directories)**" to prevent Trend Micro from scanning GFC related directories:

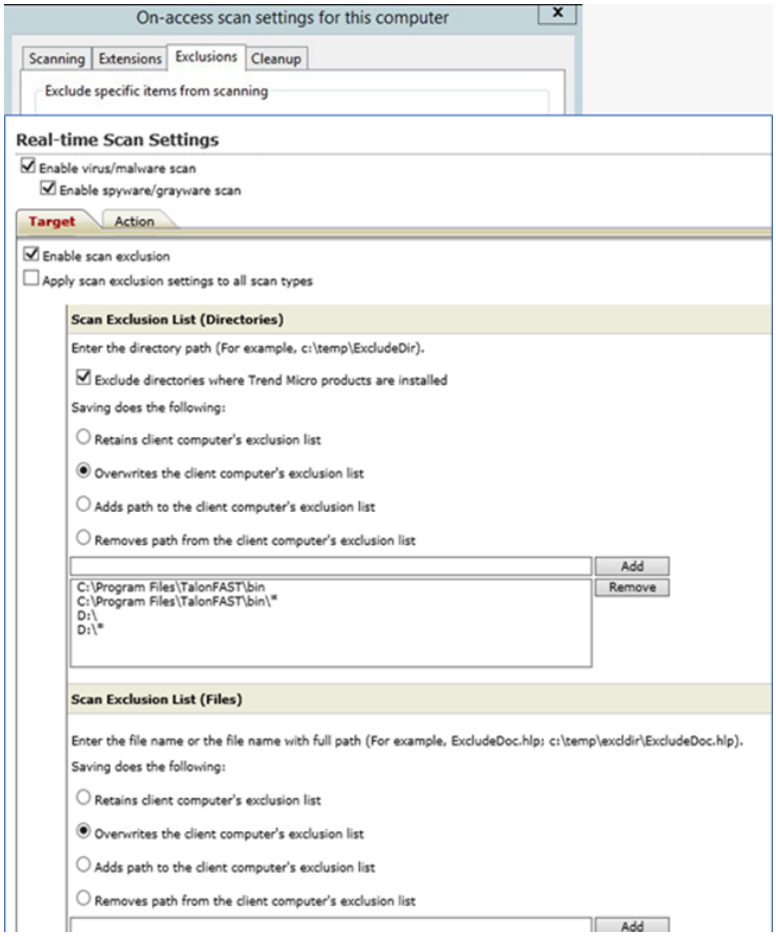
```
C:\Program Files\TalonFAST\bin\*
C:\Program Files\TalonFAST\bin
D:\*
D:
\\?\TafsMtPt:\ or \\?\TafsMtPt*
\Device\TalonCacheFS
```

5. Trend Micro will scan active processes before performing a folder/file scan. Scroll down and add the following exclusions to "**Scan Exclusion List (Files):"**

```
C:\Program Files\TalonFAST\Bin\*.exe
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\tfs.exe
C:\Program Files\TalonFAST\Bin\TService.exe
C:\Program Files\TalonFAST\Bin\tum.exe
C:\Windows\System32\drivers\tfast.sys
```

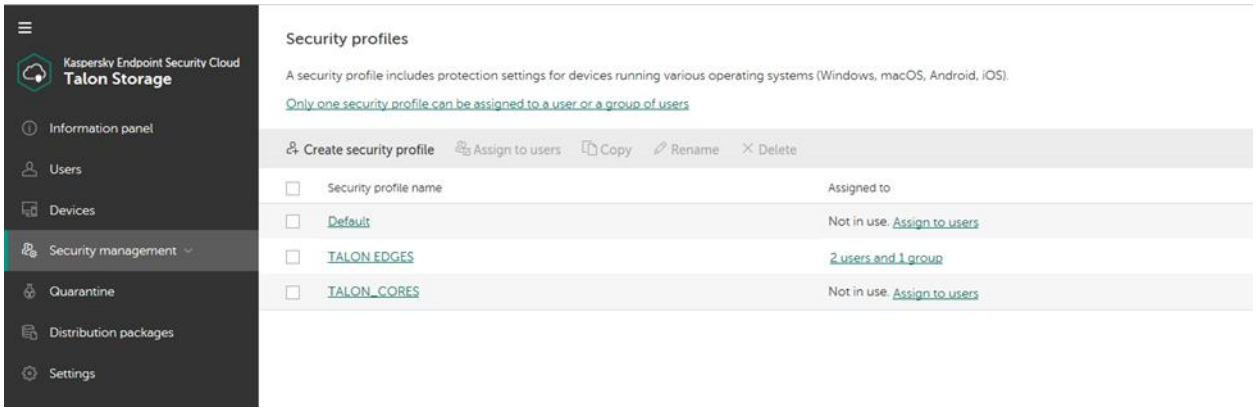

© 2020 NetApp, Inc. All Rights Reserved.

```
\\?\TafsMtPt:\ or \\?\TafsMtPt*
\Device\TalonCacheFS\
C:\Program Files\TalonFAST\FastDebugLogs\
```



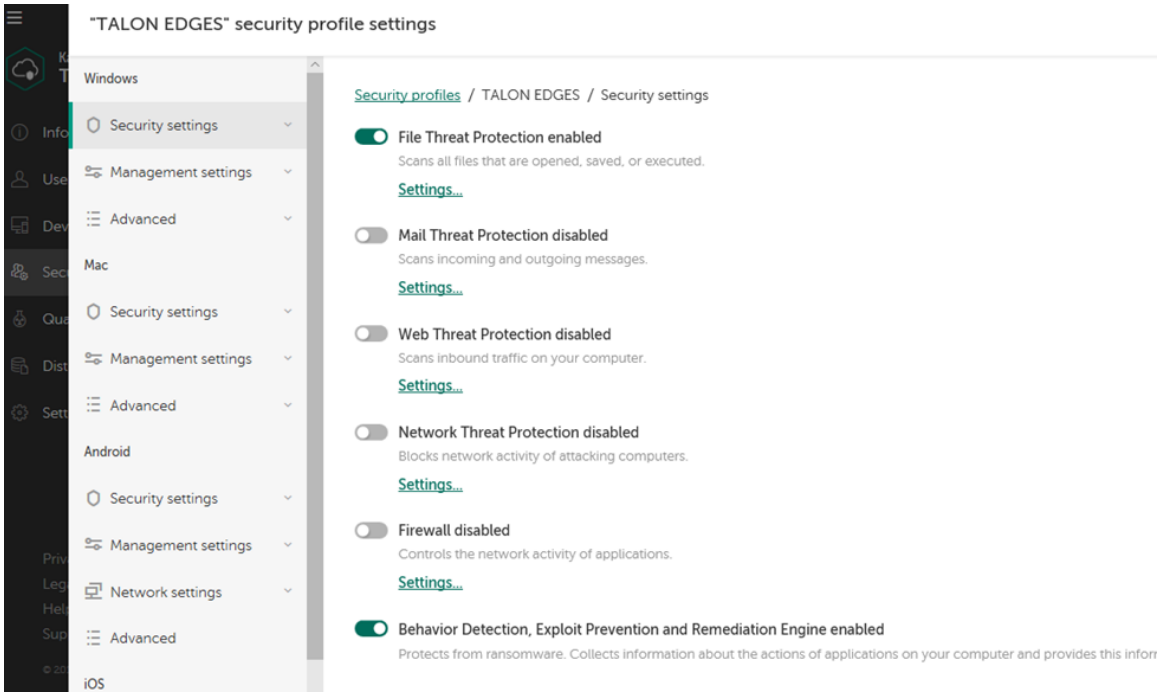
Kaspersky Endpoint Security Cloud

1. Open the Management GUI and navigate to “**Security Management**” -> “**Security Profiles**”.
2. Create a Separate GFC Edge Object OU in Kaspersky Console.

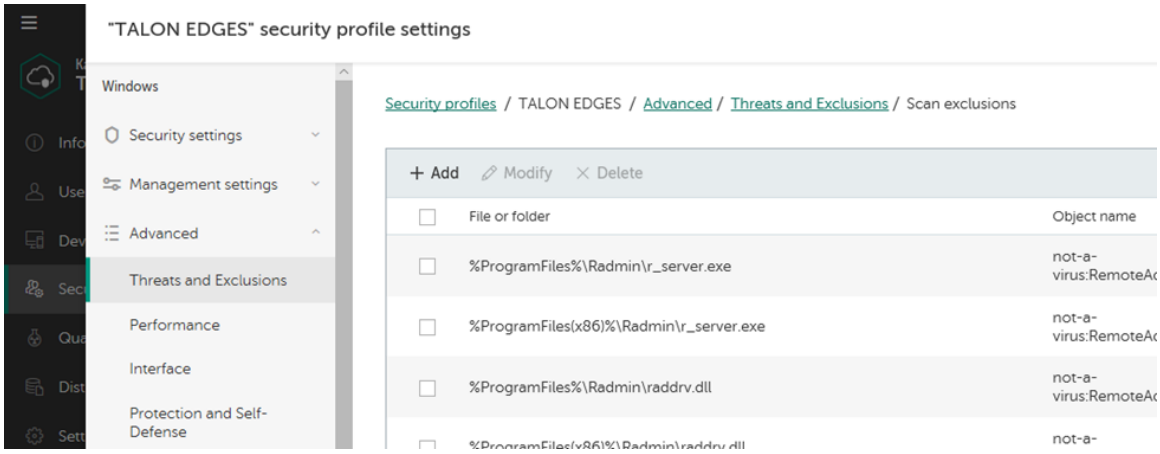


© 2020 NetApp, Inc. All Rights Reserved.

3. For the Security settings disable modules not related to file services. Only the following should be active:
   a. “File Threat Protection”
   b. “Behavior Detection, Exploit Prevention, and Remediation Engine”



4. Under “**Threats and Exclusions**” add the Folders / Files for the GFC Services



5. following exclusions to “**Scan Exclusion List (Files):”**

```
D:\
D:\LocalFASTData
C:\Program Files\TalonFAST\Bin\*.exe
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
```

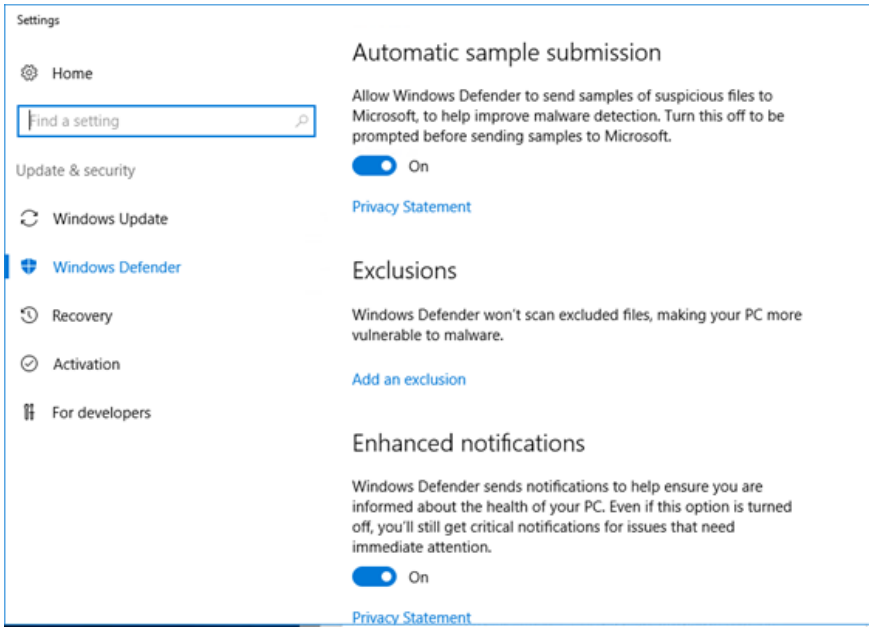

© 2020 NetApp, Inc. All Rights Reserved.

```
C:\Program Files\TalonFAST\Bin\tafsutils.exe
C:\Program Files\TalonFAST\Bin\tapp.exe
C:\Program Files\TalonFAST\Bin\tfs.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*
\\?\GLOBALROOT\Device\TalonCacheFS\
\\?\GLOBALROOT\Device\TalonCacheFS\*
Tum.exe
Tapp.exe
```

Note: The Edges should have the updated policy prior to any users begin working within the GFC Fabric.

Windows Defender

1. Open the Windows Defender Settings and under "**Exclusions**" click "**Add an Exclusion**".

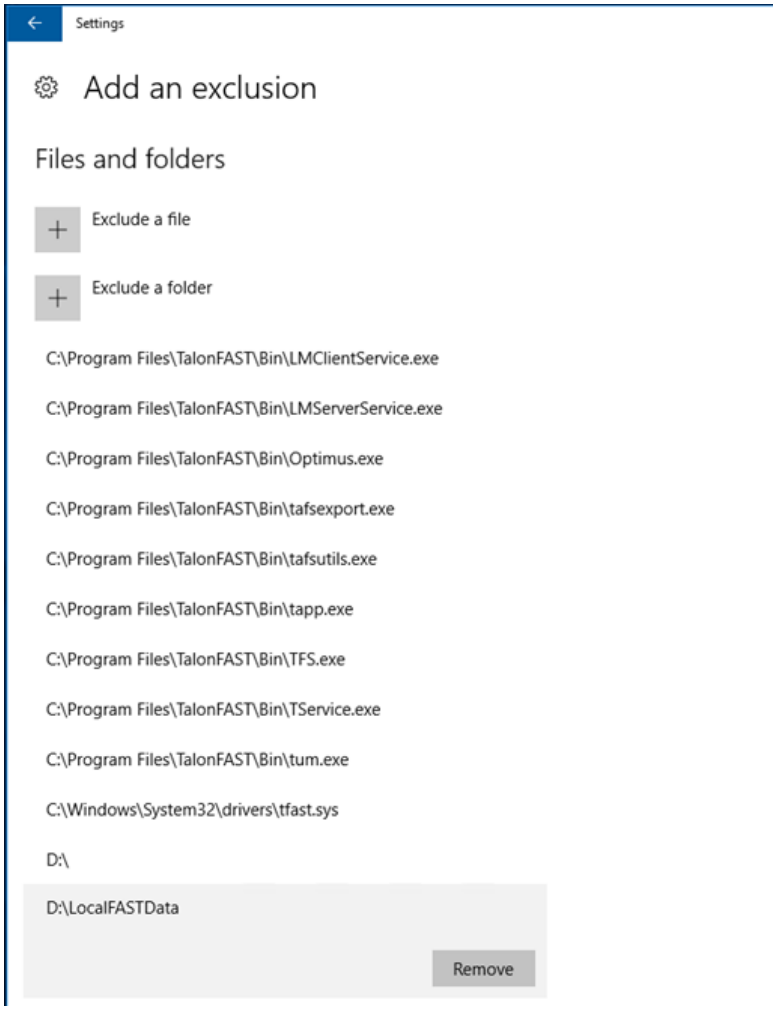


2. Under "**Files and folders**" add the GFC exclusions

```
D:\
D:\LocalFASTData
C:\Program Files\TalonFAST\Bin\*.exe
C:\Program Files\TalonFAST\Bin\LMClientService.exe
C:\Program Files\TalonFAST\Bin\LMServerService.exe
```

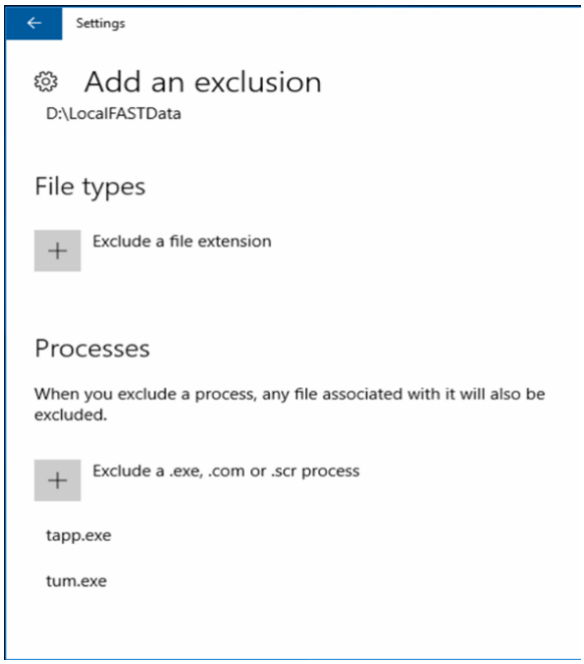

© 2020 NetApp, Inc. All Rights Reserved.

```
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\tfs.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
```



3. Under “**Processes**” exclusions add the following exclusions:
   a. Tum.exe
   b. Tapp.exe

© 2020 NetApp, Inc. All Rights Reserved.



© 2020 NetApp, Inc. All Rights Reserved.

Appendix B: Disable VMware ESX(i) Hot Plug Capability

GFC does not support caching of files and data on removable drives. Certain versions of VMware ESX will present hard disks as HotPlug/HotADD by default which Windows Server will define as “Removable.” This default behavior can be modified by editing the virtual machine’s .vmx file or within the vSphere Client.

To Disable HotPlug Capability Using the vSphere Client

1. Connect to the ESXi/ESX host or vCenter Server using the vSphere Client.
2. Power off the virtual machine.
3. Right-click the virtual machine and click “**Edit Settings**”.
4. Click the “**Options**” tab.
5. In the “**Advanced**” section, click “**General**”.
6. Click the “**Configuration Parameters**” Button.
7. Click the “**Add Row**” button.
8. Insert a new row with the name devices.hotplug and a value of “**false**”.
9. Power on the virtual machine.

To Disable HotPlug Capability Using the vSphere Web Client

1. From a web browser, connect to the vSphere Web Client.
2. Log in with Administrator credentials.
3. Navigate to the virtual machine you want to modify.
4. Right-click the virtual machine and select “**Edit Settings**”.
5. Click the “**VM Options**” tab.
6. In the “**Advanced**” section, click “**General**”.
7. Click “**Edit Configuration**”.
8. Click “**Add Row**”.
9. Insert a new row with the name devices.hotplug and a value of “**false**”.
10. Power on the virtual machine.

To Disable HotPlug Capability by Editing the Virtual Machine’s .vmx File

1. Power off the virtual machine.
2. Access the ESXi/ESX service console using an SSH client.
3. Open the virtual machine configuration file (.vmx) in a text editor. The default location is:
   `/vmfs/volumes/datastore_name/vm_name/vm_name.vmx`
4. Add the line:
   devices.hotplug = "false"
   Note: This setting does not interfere with HotPlug CPU/memory.
5. Save and close the file.
6. Power on the virtual machine.

© 2020 NetApp, Inc. All Rights Reserved.

Appendix C: NetApp Global File Cache (GFC) PowerShell Configuration

GFC Optimus PSM

Software Requirements

- Windows PowerShell 5.x (Administration / Elevated Permissions)
- Windows Management Framework 5.x
- GFC

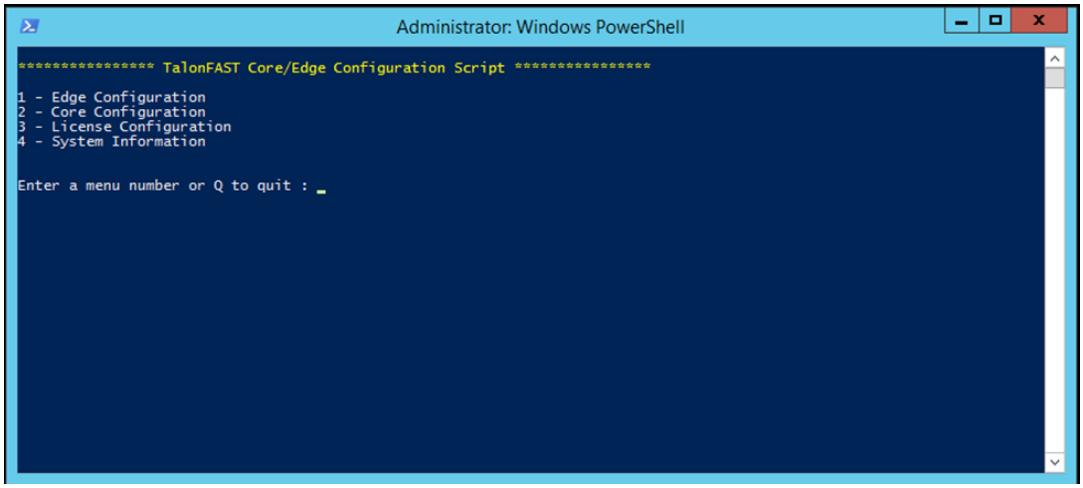
Launch GFC PowerShell Configuration CLI

To launch PowerShell configuration UI, give below command in PowerShell window. This will launch below UI.

```
&"C:\Program Files\TalonFAST\Bin\TalonFASTConfig.ps1"
```

Menu:

Figure 39)



Configuration Process

GFC configuration distributed in below sections:

- Edge Configuration
- Core Configuration
- License Configuration
- System Information

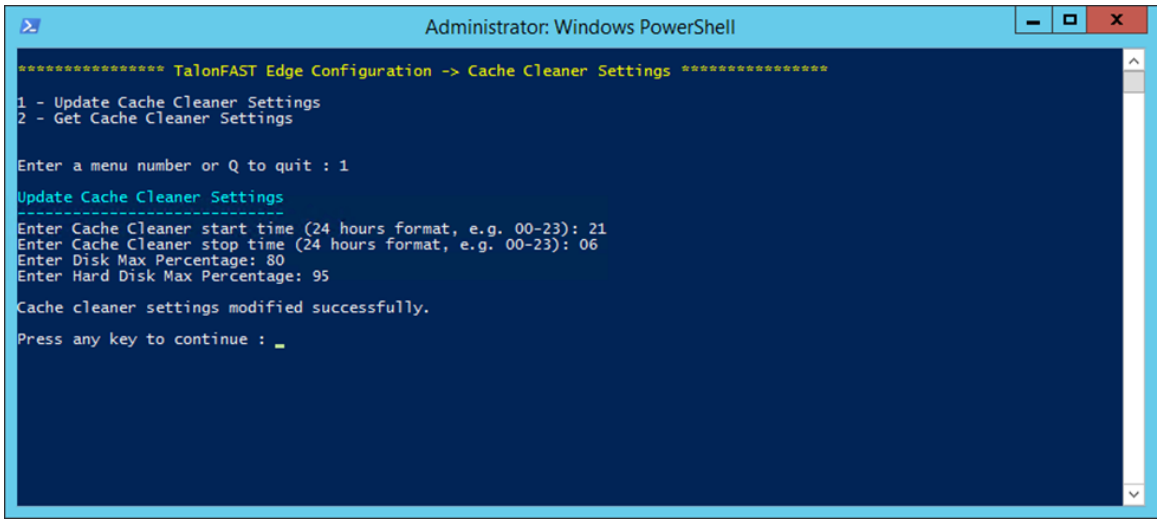
Edge Configuration

Cache Cleaner Settings

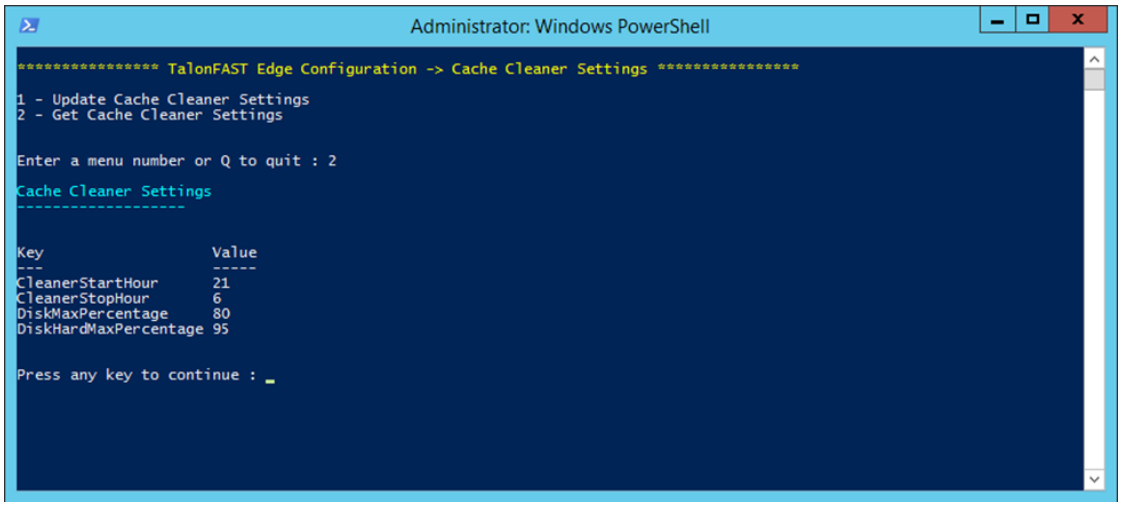
Includes following configurations settings.

1. Update Cache Cleaner Settings

© 2020 NetApp, Inc. All Rights Reserved.



2. Get Cache Cleaner Settings

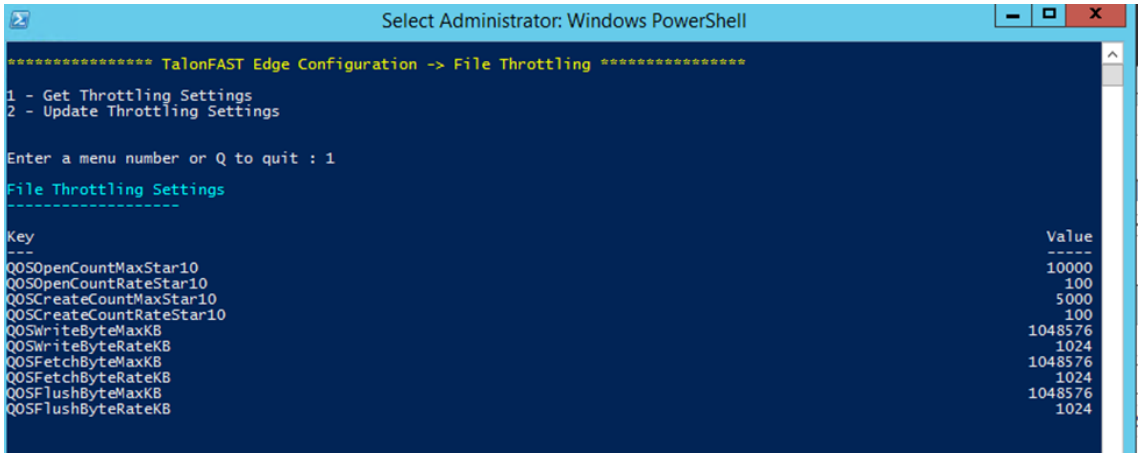


Throttling Settings

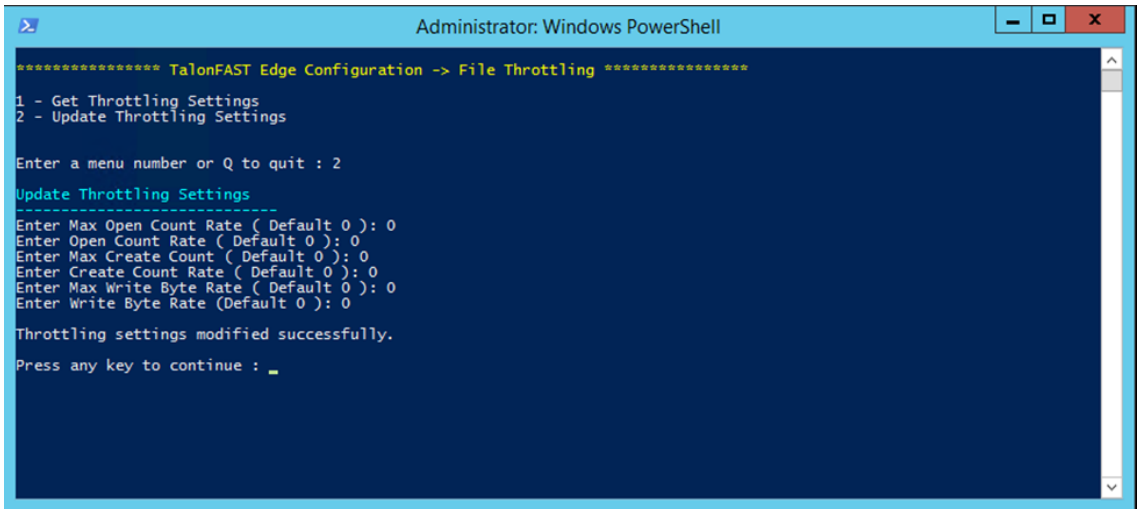
Includes following configuration settings.

1. Get Throttling Settings:

© 2020 NetApp, Inc. All Rights Reserved.



2. Update throttling settings

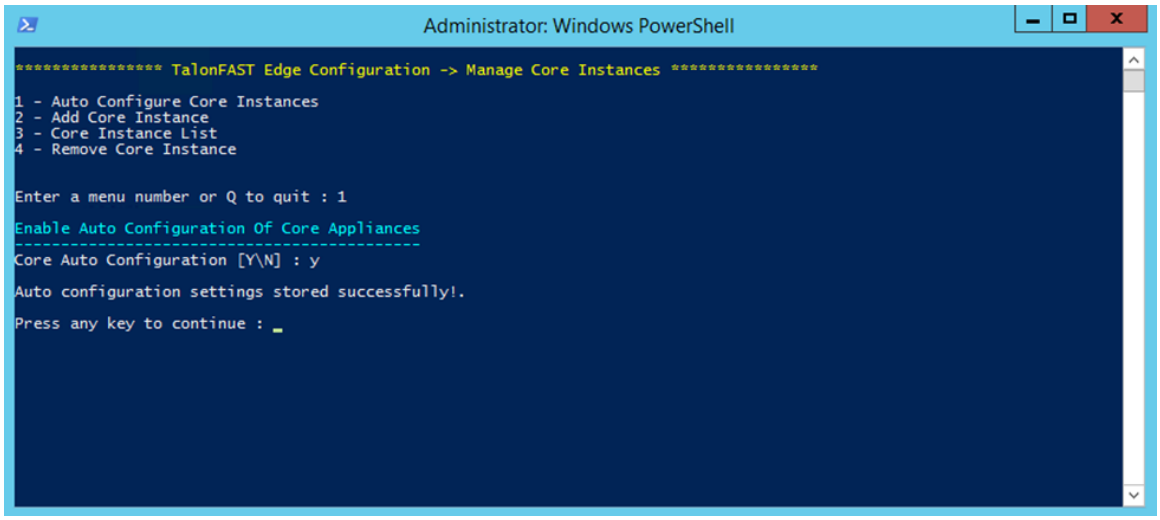


Manage Core Appliances

Manage Core Appliances which includes the below menu items:

1. Auto Configure Core Instances:

© 2020 NetApp, Inc. All Rights Reserved.



2. Add Core Instances:

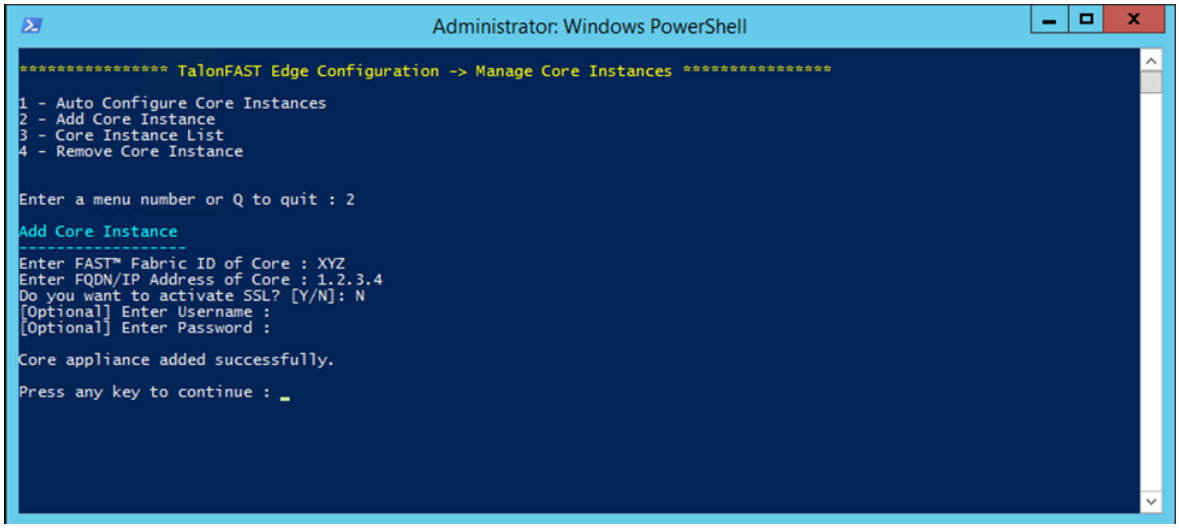
   Cloud Fabric ID: Provide the name of the GFC Fabric or datacenter location, i.e. NYC.

   FQDN / IP Address: Provide the FQDN or IP Address of GFC Fabric, i.e. 1.2.3.4.

   Enabled SSL: This is enabled when GFC edge requires SSL encryption with the GFC, i.e. when using the public internet to connect to the GFC.

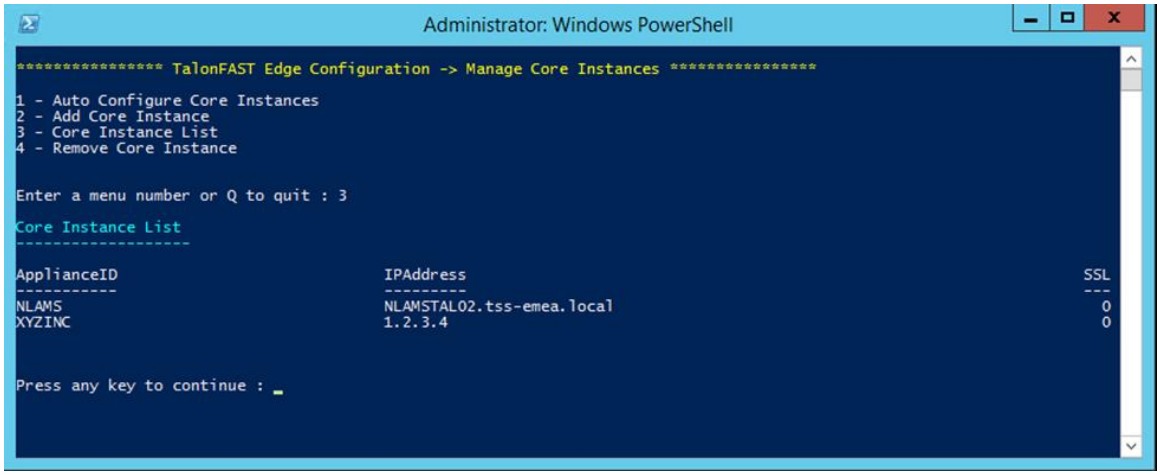
   Username: Provide designated administrative credentials to enable SSL encryption, preferably the Service Account which authenticates this GFC edge instance with the GFC Fabric, i.e. FASTAdmin.

   Password: Provide the password associated with the administrative username supplied to enable SSL encryption between the GFC edge instance and the GFC Fabric.

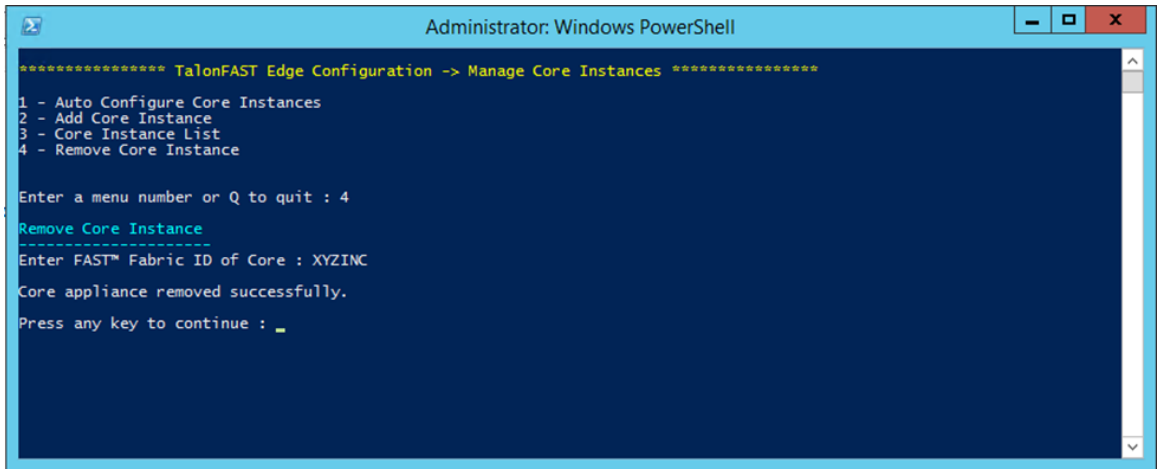


3. Core Instances List:

© 2020 NetApp, Inc. All Rights Reserved.



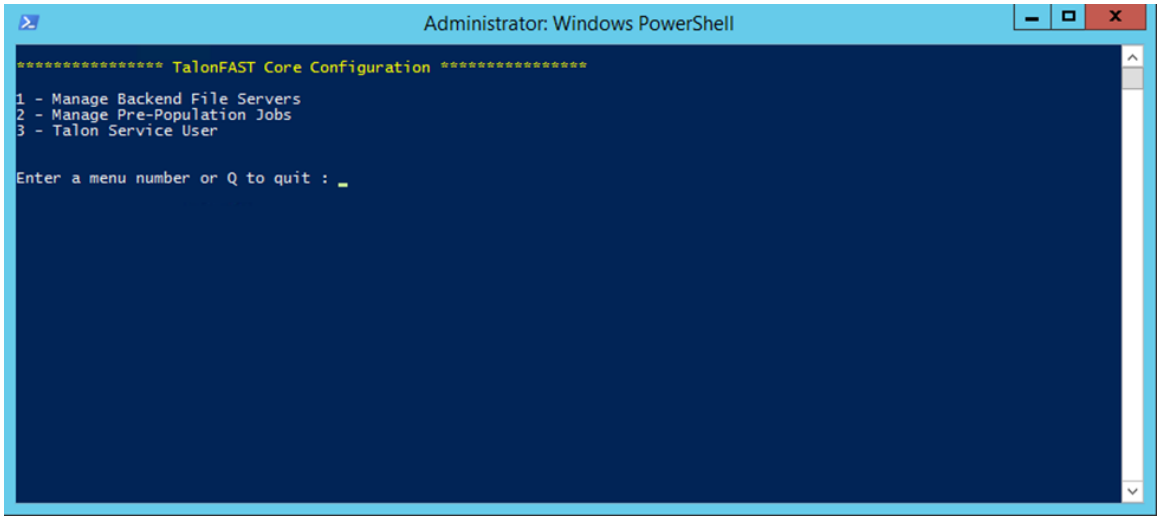
4. Remove Core Instances:



Core Configuration

Core Configuration includes the below menu items:

Figure 40)

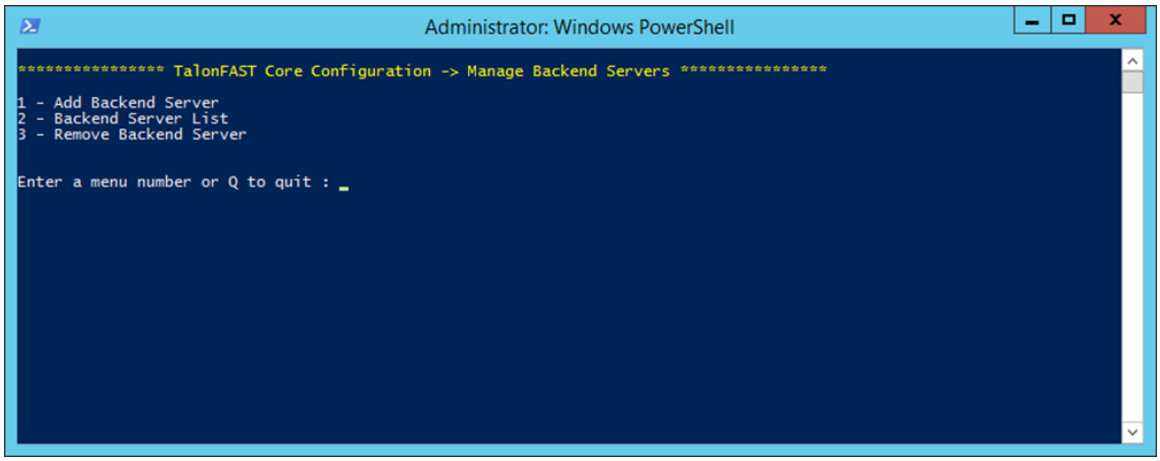


© 2020 NetApp, Inc. All Rights Reserved.

Manage Backend File Servers

Manage Backend File Servers contains the below menu items:

Figure 41)

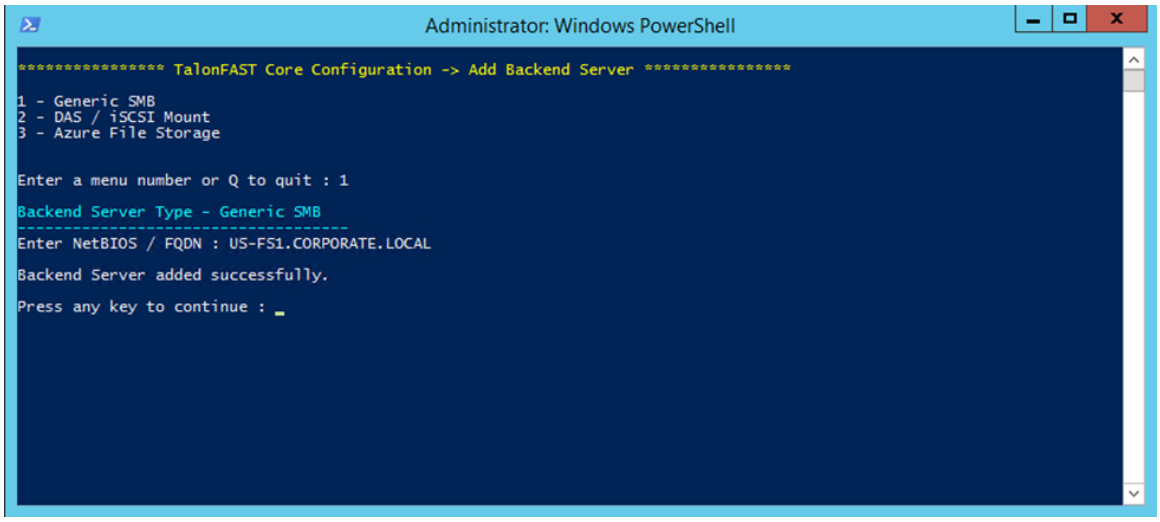


1. Add Backend Server:

There are three types of backend servers as listed below:

a. Generic SMB

NetBIOS / FQDN: Provide the NetBIOS name or FQDN of the backend file server, i.e. US-FS1 or US-FS1.CORPORATE.LOCAL

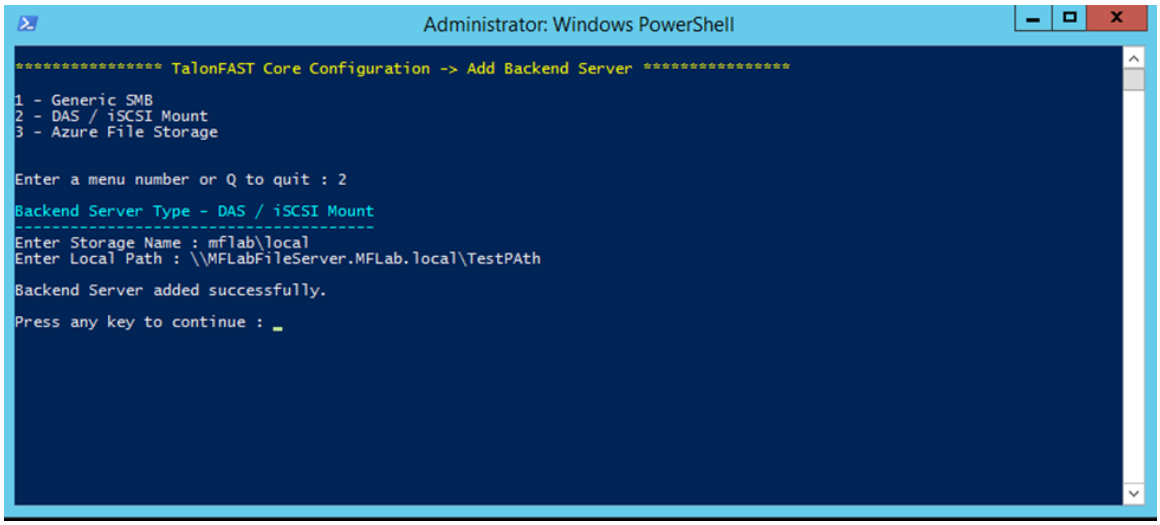


b. DAS / iSCSI Mount

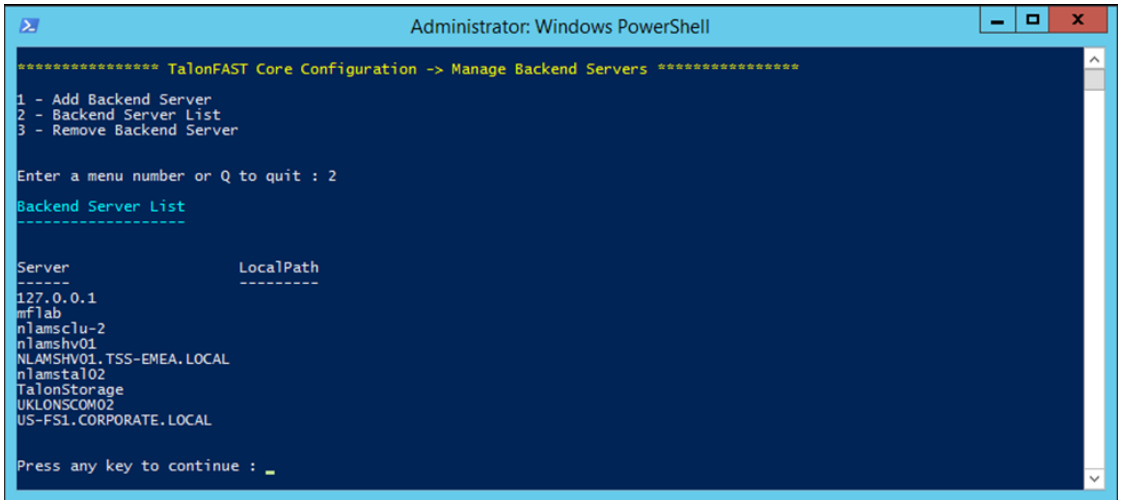
Storage Name: Provide the Storage Name which is displayed to end users in the UNC path.

LocalPath: Provide the local path of the attached storage, i.e. F:\

© 2020 NetApp, Inc. All Rights Reserved.



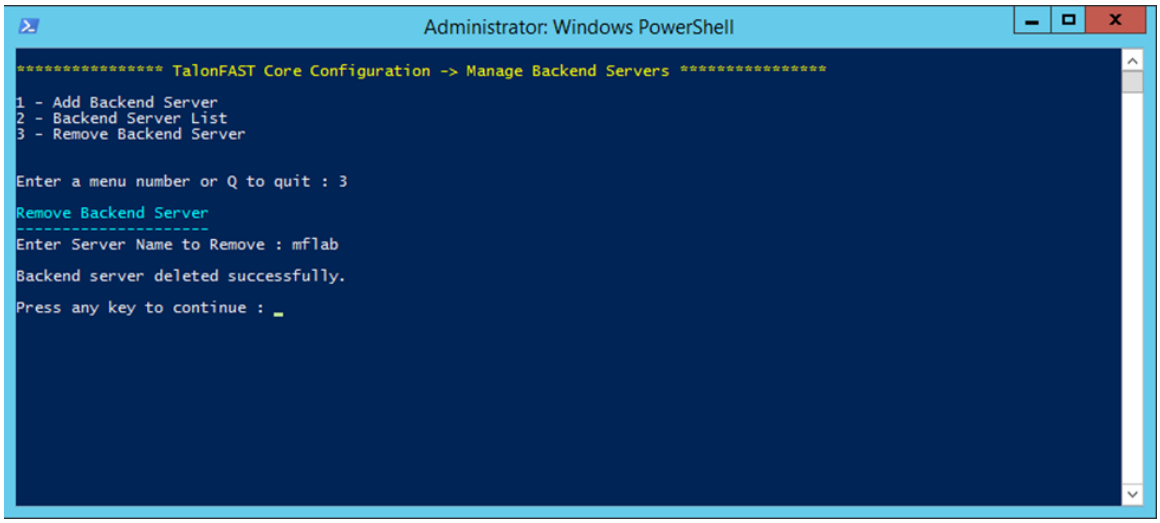
2. Backend Server List:



3. Delete Backend Server:

   Enter the name of the backend server to delete from the list.

© 2020 NetApp, Inc. All Rights Reserved.

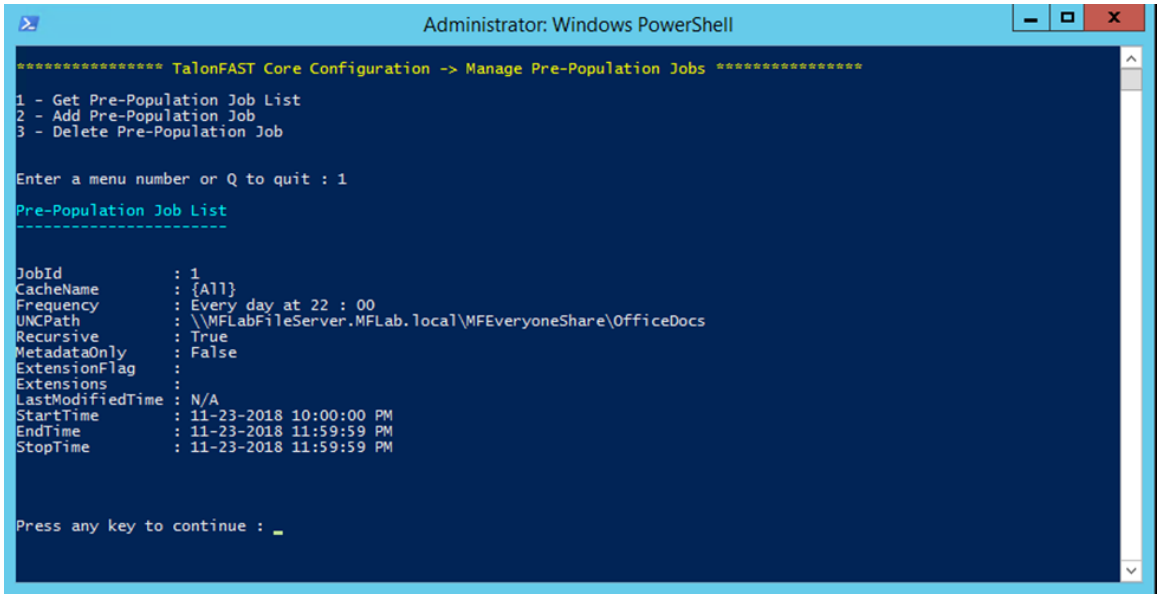


Manage Pre-Population Jobs

Manage Pre-Population contains the below menu items:

1. Get Pre-Population Job List:

   Get a list of all pre-population jobs that's have been scheduled to run



2. Add Pre-Population Job:

   Pre-population is divided into 3 components as below:

   - Path Filter Configuration
   - Frequency Configuration
   - Pre-population Job Configuration

Path Filter Configuration

These are filters added on given path, the object is saved and used for adding pre-population job. It has below parameters:

© 2020 NetApp, Inc. All Rights Reserved.

- Path: UNC path for pre-population job.
- Recursive: This filter includes all the child directories.
- MetadataOnly: It will only contain metadata file, not the actual data.
- Modified time: This will include file modified after the given time(days/hours/minutes)
- FileType: This will include or exclude the files with given extensions.

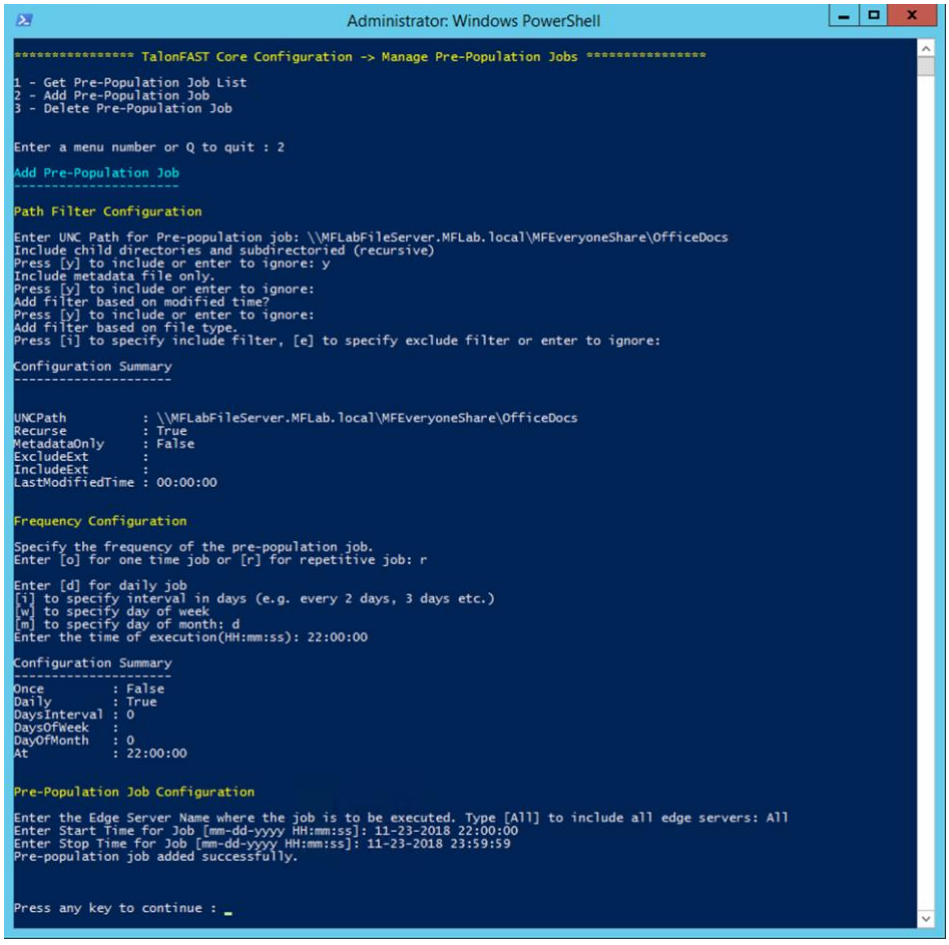
Frequency Configuration

- Specify the frequency of the pre-population Job.
- One-time job or repetitive job.
- If it's a repetitive job then select the frequency like daily, days interval, day of week, day of month
- Specify the time for the repetitive job.

Pre-Population Job Configuration

This is the final execution point where job will be added.

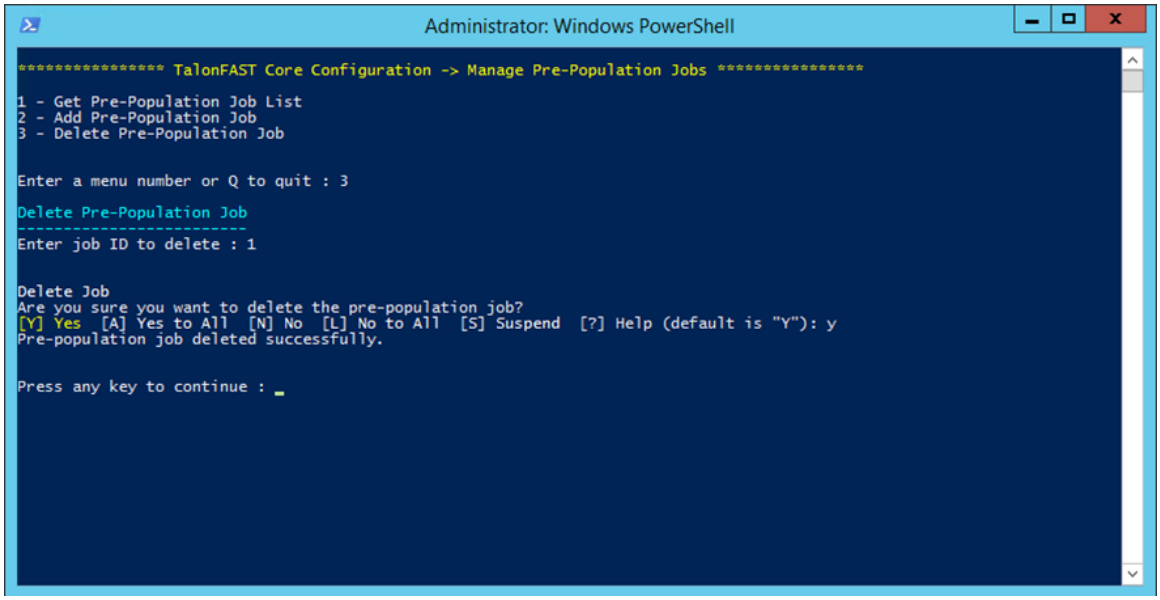
- Enter the edge server name where the job is to be executed. Job can be executed for all edge servers as well for that specify "All."
- Enter the start time for the job. If the job is repetitive then the execution time given in frequency configuration and the time for the StartTime parameter should be the same.
- Enter the stop time for the job.



© 2020 NetApp, Inc. All Rights Reserved.

3. Deleting Pre-Population Job:

   JobID: Provide the JobID of the Pre-Population job you are deleting



Advanced: Core Pre-population using PowerShell

Note: This PowerShell-based approach can only be executed from a Core instance.

Software Requirements

- Windows PowerShell 5.x (Administration / Elevated Permissions)
- Windows Management Framework 5.x
- GFC

Import GFC PowerShell Cmdlet Module

To import PowerShell cmdlets, enter the following command in the PowerShell window. The PowerShell cmdlet module contains many APIs for GFC configuration, including the cmdlet for **Add-PrePopulation Job**.

```
Import-Module "C:\Program Files\TalonFAST\Bin\OptimusPSM.dll"
```

Using Set-TLNPrePopulationPathFilter Cmdlet

Sets path filters for the pre-population job. This object can be used for multiple job creation.

```
Set-TLNPrePopulationPathFilter
-UNCPath <String>
[-Recurse]
[-MetadataOnly]
[-ExcludeExt <String[]>]
[-IncludeExt <String[]>]
[-LastModifiedTime <TimeSpan>]
```

Examples:

1. Set job as Recursive. Add parameter -Recurse

© 2020 NetApp, Inc. All Rights Reserved.

```
Set-TLNPrePopulationPathFilter -UNCPath
"\\FileServer\MFEveryoneShare\Documents" -Recurse
```

2. Set job as MetadataOnly. Add parameter -Metadataonly

```
Set-TLNPrePopulationPathFilter -UNCPath
"\\FileServer\MFEveryoneShare\Documents" -Recurse -MetadataOnly
```

If the job is only for metadata files, then use “Metadata Only” parameter. You cannot set Exclude Ext, Include Ext and LastModifiedTime parameters with MetadataOnly. It will respond with an exception message if attempted.

3. Set job to filter by file types to include files of defined extensions. Add Parameter -IncludeExt [.ext1, .ext2, .ext3]

```
Set-TLNPrePopulationPathFilter -UNCPath
"\\FileServer\MFEveryoneShare\Documents" -Recurse -IncludeExt .txt, .docx,
.pptx
```

4. Set job to filter by file types to exclude files of defined extensions. Add parameter -ExcludeExt [.ext1, .ext2, .ext3]

```
Set-TLNPrePopulationPathFilter -UNCPath
"\\FileServer\MFEveryoneShare\Documents" -Recurse -ExcludeExt .txt, .docx,
.pptx
```

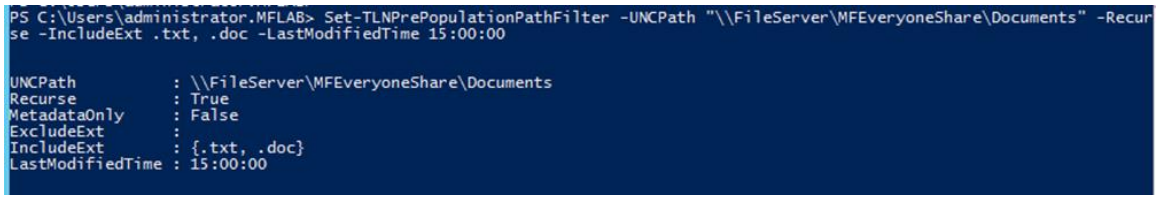
IncludeExt and ExcludeExt cannot be used for same filter. Use either IncludeExt or ExcludeExt, otherwise it will output an ArgumentException.

5. Only include files modified with the defined timespan. Add parameter -lastmodifiedtime

```
Set-TLNPrePopulationPathFilter -UNCPath
"\\FileServer\MFEveryoneShare\Documents" -Recurse -LastModifiedTime
15:00:00
```

This cmdlet returns an object of PathFilter which will be displayed similar to the below:

Figure 42)



Using Set-TLNPrePopulationFrequency Cmdlet

This sets the frequency for the pre-population job which is the execution schedule for the job. This cmdlet output is a mandatory parameter for adding a pre-population job. All parameters are basically a type of frequency for execution.

```
Set-TLNPrePopulationFrequency
[-Once]
[-Daily]
[-DaysInterval <UInt32>]
[-DaysOfWeek <DayOfWeek[]>]
[-DayOfMonth <Uint32>]
[-At <TimeSpan>]
```

Examples:

1. To execute a job only once set -Once parameter. Add parameter -Once

© 2020 NetApp, Inc. All Rights Reserved.

```
Set-TLNPrePopulationFrequency -Once
```

If the job is going to be a OneTime job then, then this parameter is mandatory. Other parameters for recurring jobs are not allowed with this type of frequency.

2. Executing job on Daily Basis. Add parameter -Daily

```
Set- TLNPrePopulationFrequency -Daily -At 16:00:00
```

To execute daily jobs, the -Daily parameter needs to be set. If using the -Daily parameter, using -At is also required to set the time at which job will be executed.

3. Executing jobs on interval basis. Add Paramteter -DaysInterval

```
Set- TLNPrePopulationFrequency -DaysInterval 3 -At 12:30:00
```

The above example job will execute every 3 days at 12.30 PM local time. Other parameters are not allowed for this type, which will return an exception message.

4. Set the job on a weekly basis. Add parameter -DayOfWeek

```
Set- TLNPrePopulationFrequency -DaysOfWeek Friday -At 18:30:00
```

This job will execute every Friday at 6.30 PM.

5. Set the job frequency to a day of the month. Add parameter -DayOfMonth

```
Set- TLNPrePopulationFrequency -DayOfMonth 15 -At 15:00:00
```

The above job will be executed on the 15th of every month at 3:00 PM.

This cmdlet returns an object of Frequency which will be displayed like the example below:

Figure 43)

```
PS C:\Users\administrator.MFLAB> Set-TLNPrePopulationFrequency -Daily -At 14:45


Once         : False
Daily        : True
DaysInterval : 0
DaysOfWeek   :
DayOfMonth   : 0
At           : 14:45:00
```

Using Add-TLNPrePopulationJob Cmdlet

To finish the process, this is the main cmdlet which creates a new pre-population job.

```
Add-TLNPrePopulationJob
[-AllEdgeServers]
[-EdgeServers <String[]>]
-StartTime <DateTime>
-StopTime <DateTime>
-Filter <PSobject>
-Frequency <PSObject>
```

Examples:

1. To execute job for all edge servers. Add Parameter -AllEdgeServers

```
Add-TLNPrePopulationJob -AllEdgeServers -StartTime "01-11-2018 14:45:00" -
StopTime "01-31-2018 18:00:00" -Filter $objFilter -Frequency $objFrequency
```

This will create a job for all Edge instances connected to a Core. -Filter and -Frequency Powershell Objects need to pass to this cmdlet which are mandatory parameters.

2. To execute a job on one or more Edge Servers, Add Parameter –EdgeServers [1,2,3]

© 2020 NetApp, Inc. All Rights Reserved.

```
Add-TLNPrePopulationJob -EdgeServers EDGESERVER1, EDGESERVER2, EDGESERVER3
-StartTime "01-11-2018 14:45:00" -StopTime "01-31-2018 18:00:00" -Filter
$objFilter -Frequency $objFrequency
```

This will create a job on one or more Edge instances connected to a Core. Edge Servers is a string array, so it is possible to add multiple Edge instances.

End-to-end Example of Cmdlet

For the Add-TLNPrePopulation Job cmdlet, a complete example may look like the following using the previously detailed Cmdlets:

```
$objFilter = Set-TLNPrePopulationPathFilter -UNCPath "\\FileServer.local\MFEveryOneShare" -
Recurse -IncludeExt .jpeg, .txt, .docx
$objFilter
$objFrequency = Set-TLNPrePopulationFrequency -Daily -At 14:45
$objFrequency
Add-TLNPrePopulationJob -EdgeServers EDGESERVER1, EDGESERVER2 -StartTime "01-11-2018 14:45:00" -
StopTime "01-31-2018 18:00:00" -Filter $objFilter -Frequency $objFrequency
```

Below is a breakdown of the example provided above.

Note: Add-TLNPrepopulationJob needs to be detailed, as running that command WILL force prompts to fill out the offsets/switches for Pre-Population.

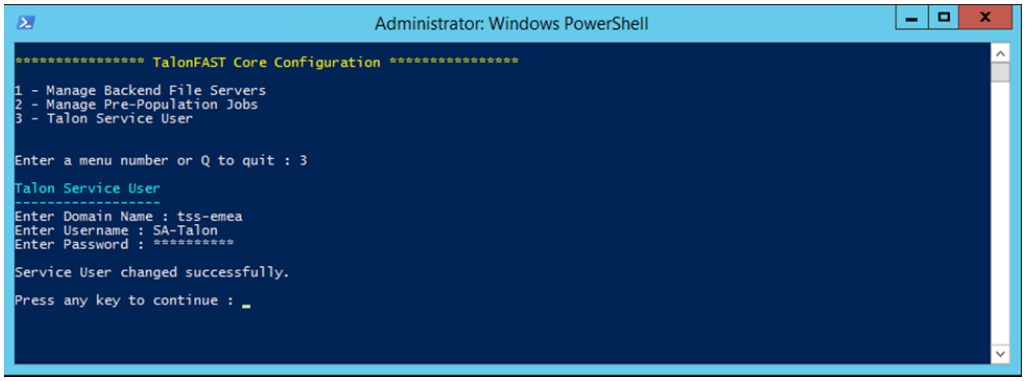
Service Account

Configure Core instance Service Account with below parameters.

Username: Provide the Service Account username that will be used to start the GFC service. Note that this service account must be a member of the local backup operators' group or local administrators' group on the backend file server. See the GFC user guide for further information.

Password: Provide the password for the Service Account.

Figure 44)

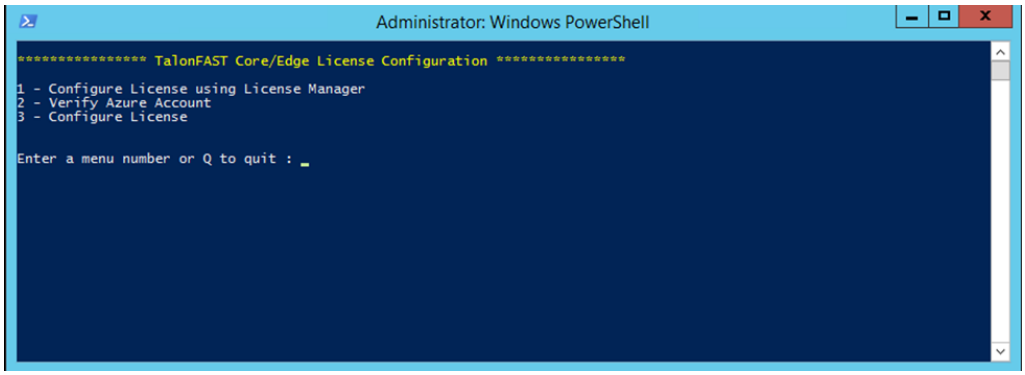


License Configuration

License Configuration includes below menus.

© 2020 NetApp, Inc. All Rights Reserved.

Figure 45)

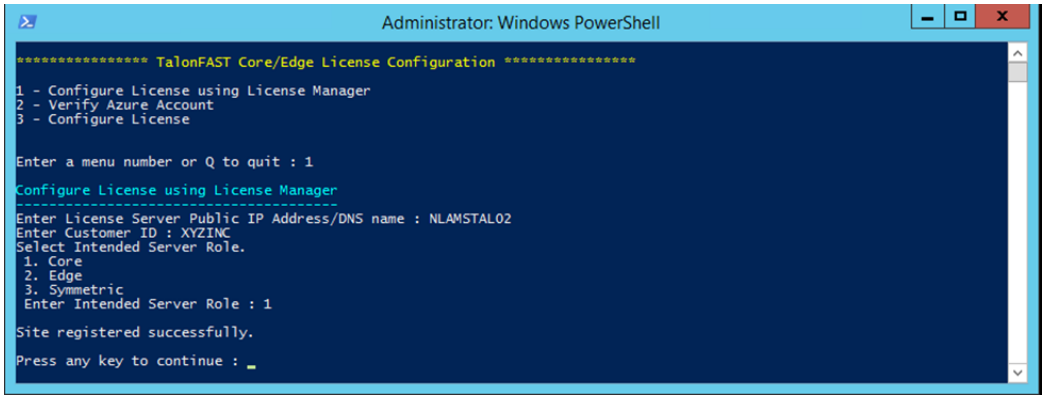


1. Configure License using License Manager:

   License Server Public IP Address/DSN Name: Provide the FQDN or IP address of the GFC instance that has been deployed as central license manager server, i.e. 1.2.3.4

   Customer ID: Provide the customer identifier, as provided by NetApp Support services, to associate this instance with your license manager server.

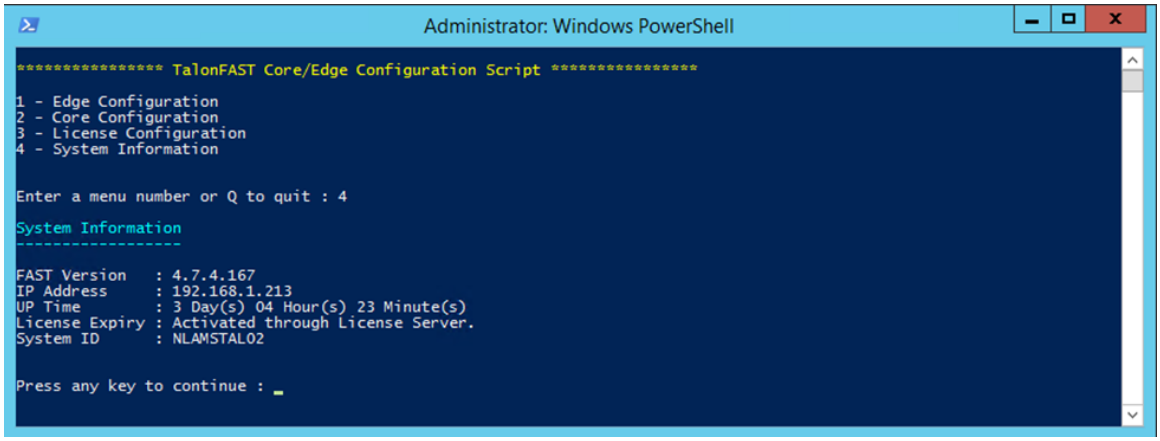
   Intended Server Role: Select the role of the GFC instance which can be Core, Edge or Symmetric.



System Information

Provides the server details.

Figure 46)



© 2020 NetApp, Inc. All Rights Reserved.

GFC Namespace for TUMMIProvider

The recently added TUMMIProvider give customers the ability to manage their GFC infrastructure through a number of PowerShell commands. These have been broken up into the two primary modes of operation for the TUM Service, TUM.exe -s “Server / Core” and TUM.exe -c “Client / Edge”. In this section a command and their output examples will be provided for each scenario where these may be utilized.

Note: Prior to utilizing these scripts you should discuss this with the NetApp Support team for the most effective utilization.

TUMMIProvider is divided into two namespaces as below:

- root\TalonMIProviderv1\Core
- root\TalonMIProviderv1\Edge

To run TUMMIProvider cmdlets:

For Core instances, ensure the namespace is defined with root\TalonMIProviderv1\Core

For Edge instances, ensure the namespace is defined with root\TalonMIProviderv1\Edge

e.g.

GFC Core: Get-WmiObject -Namespace root\TalonMIProviderv1\Core -Class TLN_TUMSettings

GFC Edge: Get-WmiObject -Namespace root\TalonMIProviderv1\Edge -Class TLN_TUMSettings

Below is a list of classes within the TUMMIProvider:

- TUM Settings
- Lease Manager
- DBG Commands
- Bulk Statistics
- New Bulk Statistics
- RPC Statistics
- Dirty Files
- Active Fetches
- Active Flushes

TUM Settings

The TUM Settings provide the ability to view the details of the GFC server that has been provisioned. This can also allow for adjustments to Debug Level on a specific server for advanced troubleshooting.

1. Get instance of TUM Settings

   Core Command:

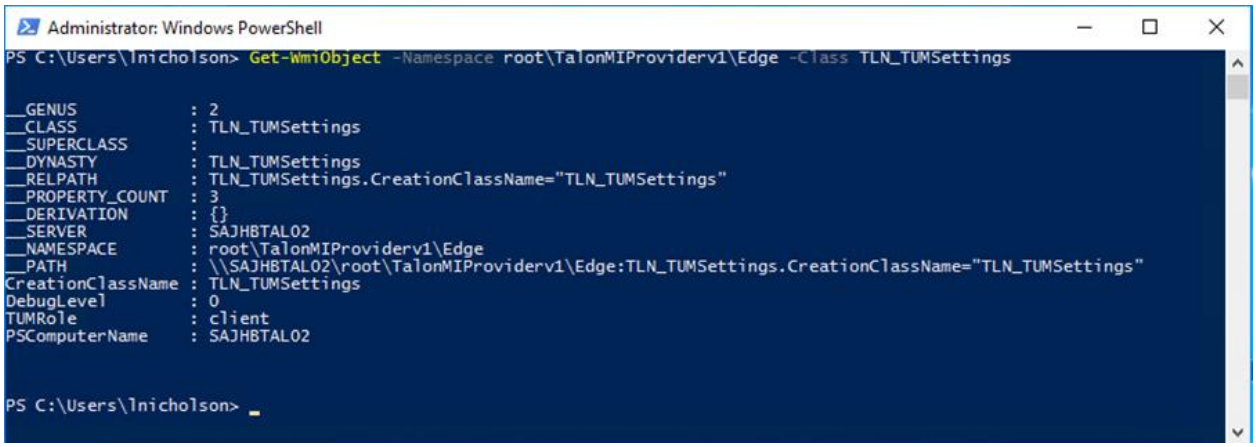
   ```
   Get-WmiObject -Namespace root\TalonMIProviderv1\Core -Class
   TLN_TUMSettings
   ```

   Edge Command:

   ```
   Get-WmiObject -Namespace root\TalonMIProviderv1\Edge -Class
   TLN_TUMSettings
   ```

   Edge Output Example:

© 2020 NetApp, Inc. All Rights Reserved.



2. Setting the Debug level

   Get instance of TLN_TUMSettings and change debug level.

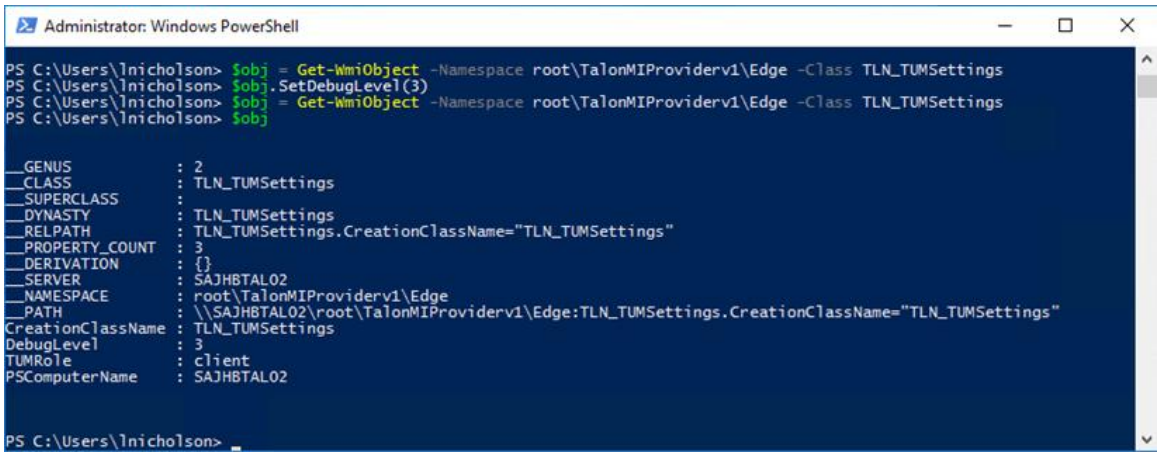
   Core Command:

```
$obj = Get-WmiObject -Namespace root\TalonMIProviderv1\Core -Class TLN_TUMSettings
$obj.SetDebugLevel(3)
$obj = Get-WmiObject -Namespace root\TalonMIProviderv1\Core -Class TLN_TUMSettings
$obj
```

   Edge Command:

```
$obj = Get-WmiObject -Namespace root\TalonMIProviderv1\Edge -Class TLN_TUMSettings
$obj.SetDebugLevel(3)
$obj = Get-WmiObject -Namespace root\TalonMIProviderv1\Edge -Class TLN_TUMSettings
$obj
```

Edge Output Example:



Lease Manager

The lease manager scripts provide the ability to display the current leases, filter the leases to find specific open leases and revoke the lease from a specific file or set of parameters.

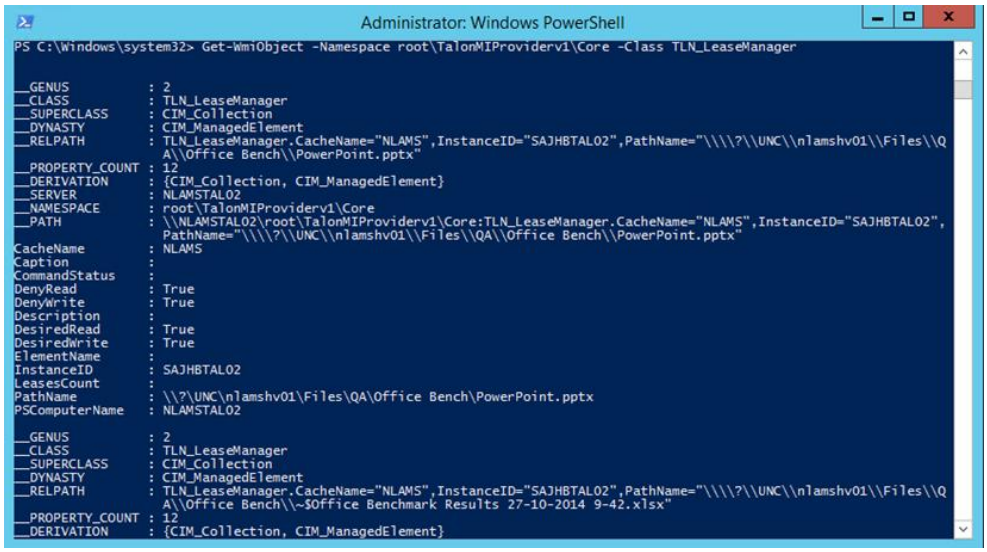
1. Get instance of TLN_LeaseManager

   Core Command:

   `Get-WmiObject -Namespace root\TalonMIProviderv1\Core -Class TLN_LeaseManager`

© 2020 NetApp, Inc. All Rights Reserved.

Output:



2. Filter instances of Lease Manager

   Filtering the leases will give you the ability to identify a specific file that may be required to be unlocked.

   The filter can be defined with any of the properties related to the leased file these properties are as follows:

   CacheName, Caption, CommandStatus, DenyRead, DenyWrite, Description, DesiredRead, DesiredWrite, ElementName, InstanceID, LeaseCount, PathName, PSComputerName.

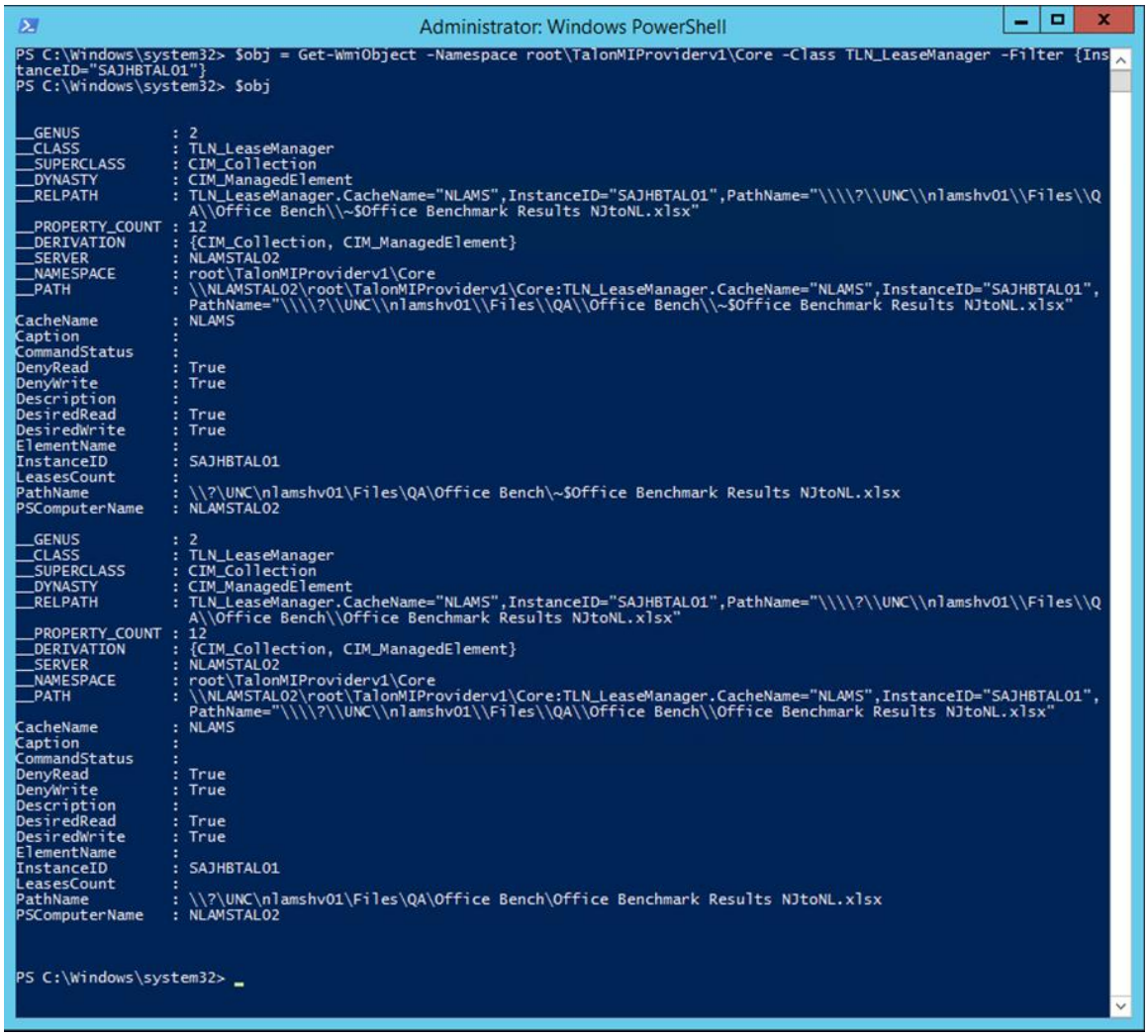
   Replace '\' with '\\' while filtering with pathname.

   Core Command:

   ```
   $obj = Get-WmiObject -Namespace root\TalonMIProviderv1\Core -Class TLN_LeaseManager -Filter {InstanceID="SAJHBTAL01"}
   $obj
   ```

Output

© 2020 NetApp, Inc. All Rights Reserved.

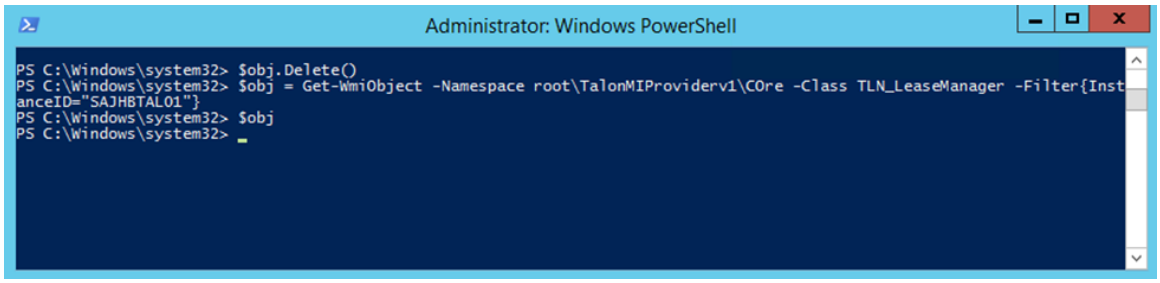


3. Deleting lease. Follow steps from step (2) and run below command.

   Core Command:

   `$obj.Delete()`

   Output



DBG Commands

The DBG Commands provides the ability to manually clear the cache based on the Least Recently Used (LRU) algorithm to clear up between 25% and 75% of the available disk space. It can also provide the

© 2020 NetApp, Inc. All Rights Reserved.

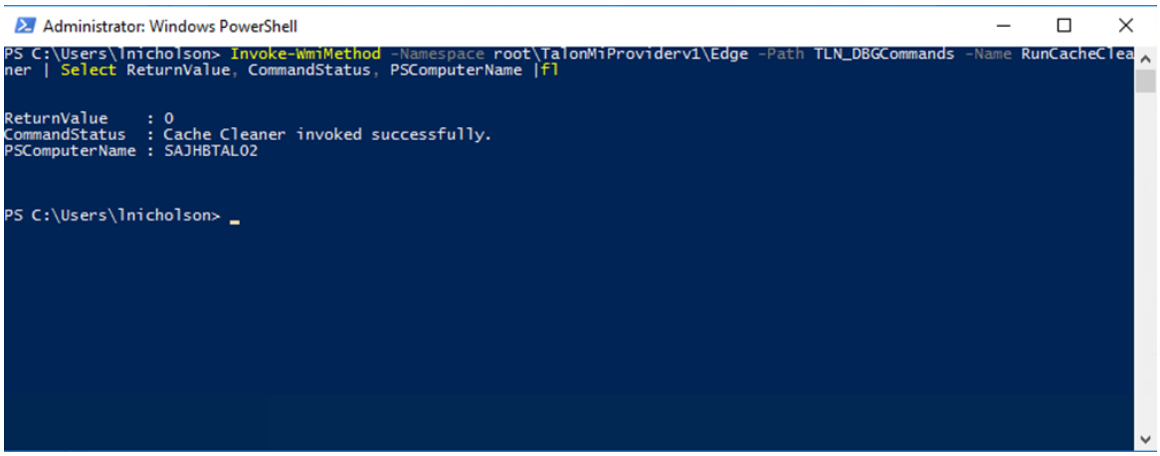
functionality to turn Toggle Event Profiling, Toggle Policy Engine Support and Toggle Light Weight Directory Support ON/OFF as required.

1. Run Cache Cleaner

   Edge Command:

   ```
   Invoke-WmiMethod -Namespace root\TalonMiProviderv1\Edge -Path
   TLN_DBGCommands -Name RunCacheCleaner | Select ReturnValue, CommandStatus,
   PSComputerName |fl
   ```

   Output



2. Toggle Event Profiling

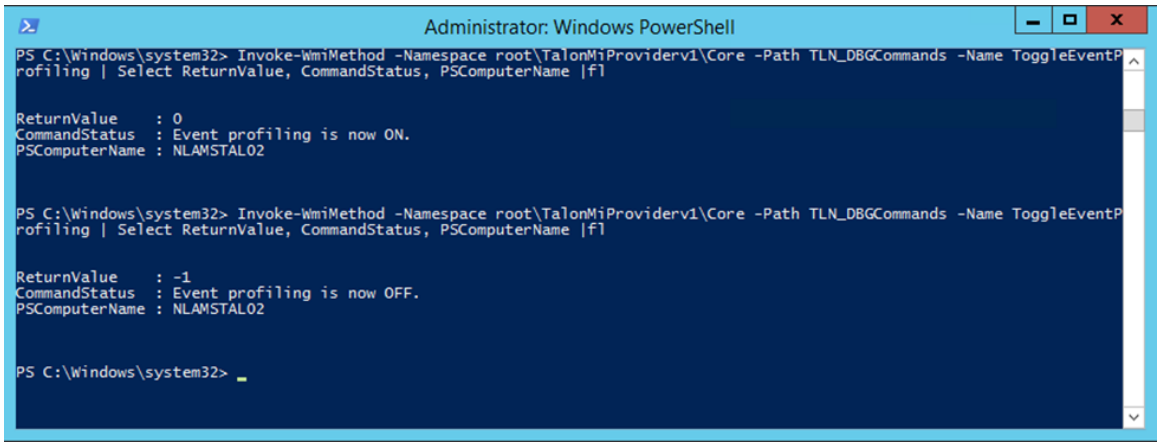
   Core Command:

   ```
   Invoke-WmiMethod -Namespace root\TalonMiProviderv1\Core -Path
   TLN_DBGCommands -Name ToggleEventProfiling | Select ReturnValue,
   CommandStatus, PSComputerName |fl
   ```

   Edge Command:

   ```
   Invoke-WmiMethod -Namespace root\TalonMiProviderv1\Edge -Path
   TLN_DBGCommands -Name ToggleEventProfiling | Select ReturnValue,
   CommandStatus, PSComputerName |fl
   ```

   Output



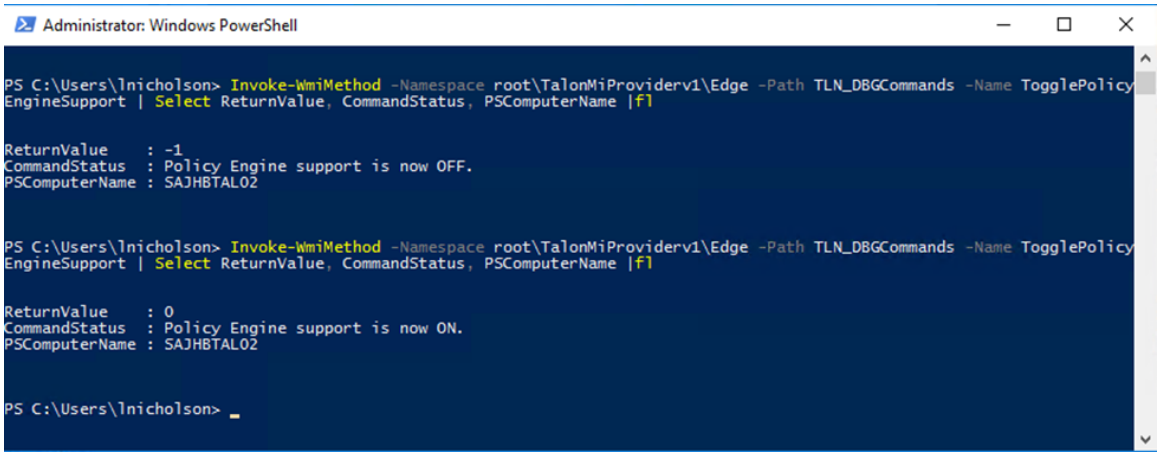
3. Toggle Policy Engine Support

   Edge Command:

© 2020 NetApp, Inc. All Rights Reserved.

```
Invoke-WmiMethod -Namespace root\TalonMiProviderv1\Edge -Path
TLN_DBGCommands -Name TogglePolicyEngineSupport | Select ReturnValue,
CommandStatus, PSComputerName |fl
```

Output:

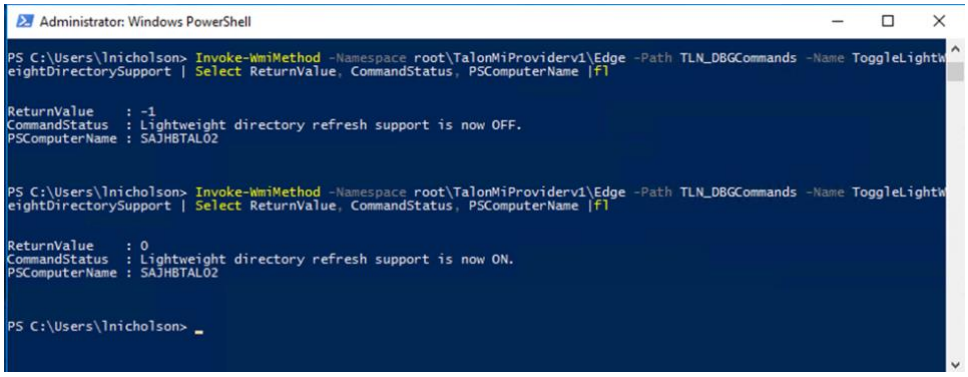


4. Toggle Light Weight Directory Support

   Edge Command:

   ```
   Invoke-WmiMethod -Namespace root\TalonMiProviderv1\Edge -Path
   TLN_DBGCommands -Name ToggleLightWeightDirectorySupport | Select
   ReturnValue, CommandStatus, PSComputerName |fl
   ```

   Output:



Bulk Statistics

The Bulk Statistics provides you with the ability to read all the statics related to the compression, streaming and delta differencing with an overall transfer efficiency percentage, this can be run from a Core or an Edge.

1. Display Bulk Statistics

   Core Command:

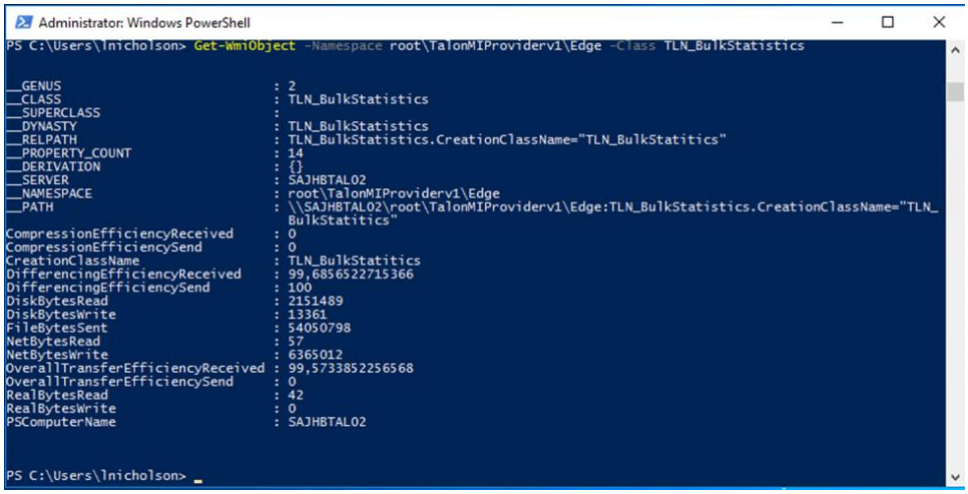
   ```
   Get-WmiObject -Namespace root\TalonMIProviderv1\Core -Class
   TLN_BulkStatistics
   ```

   Edge Command:

   ```
   Get-WmiObject -Namespace root\TalonMIProviderv1\Edge -Class
   TLN_BulkStatistics
   ```


© 2020 NetApp, Inc. All Rights Reserved.

Edge Output:



New Bulk Statistics

The new bulk statistics provide you with the latest results related to the server for viewing which can be reset giving the ability to actively monitor a specific instance in real time.

1. Display New Bulk Statistics

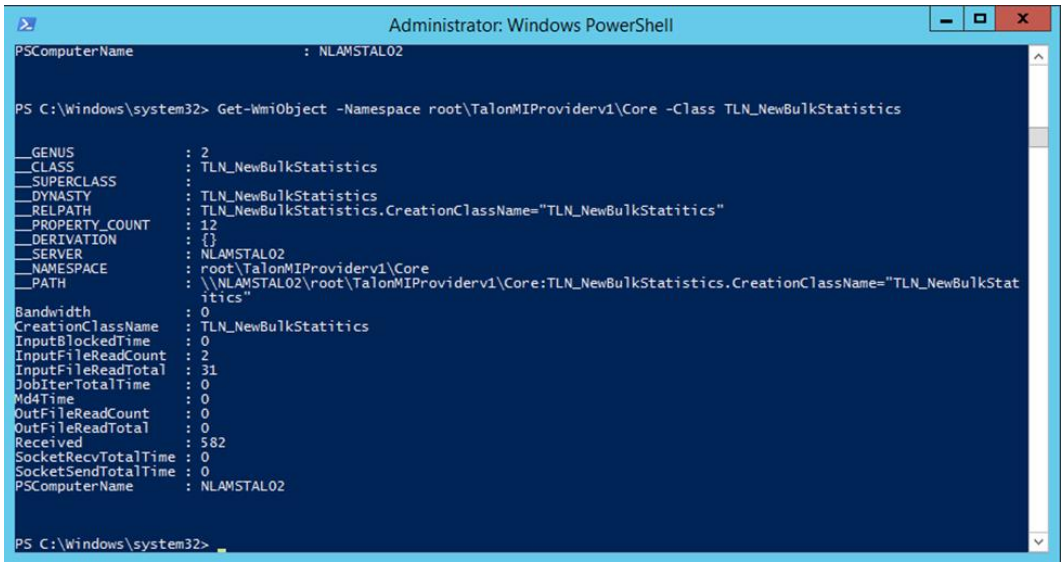
   Core Command:

   ```
   Get-WmiObject -Namespace root\TalonMIProviderv1\Core -Class
   TLN_NewBulkStatistics
   ```

   Edge Command:

   ```
   Get-WmiObject -Namespace root\TalonMIProviderv1\Edge -Class
   TLN_NewBulkStatistics
   ```

   Core Output:



2. Reset New Bulk Statistics

   Core Command:

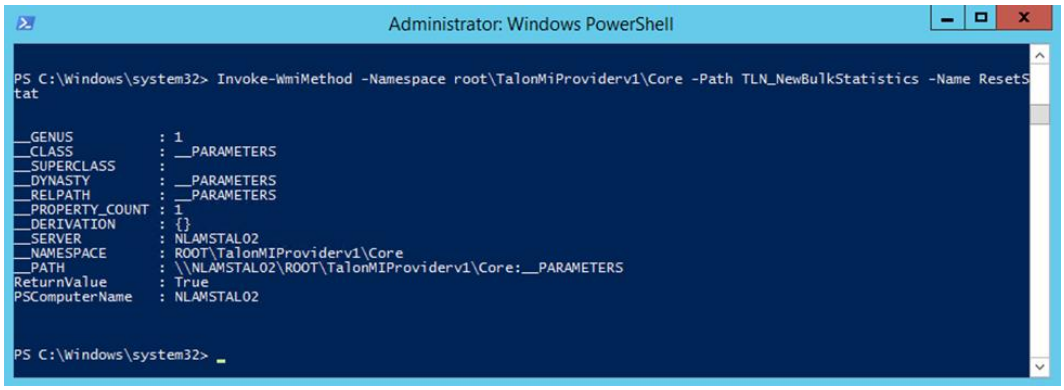
© 2020 NetApp, Inc. All Rights Reserved.

```
Invoke-WmiMethod -Namespace root\TalonMiProviderv1\Core -Path
TLN_NewBulkStatistics -Name ResetStat
```

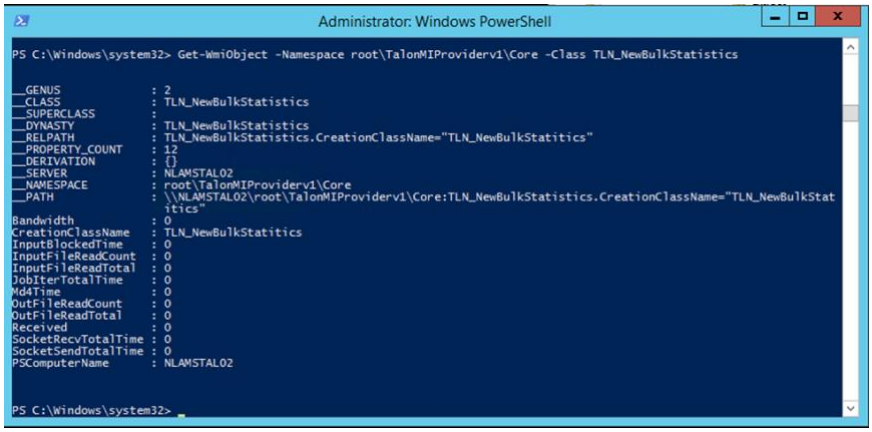
Edge Command:

```
Invoke-WmiMethod -Namespace root\TalonMiProviderv1\Edge -Path
TLN_NewBulkStatistics -Name ResetStat
```

Core Output:



3. Rerun “Display New Bulk Statistics” as per page 178:



RPC Statistics

The RPC statistics provide you with information related to the GFC Fabric on a specific machine. It gives the time in milliseconds, counts, and Average number of retries for specific RPC protocols utilized.

1. Display RPC Statistics

   Core Command:

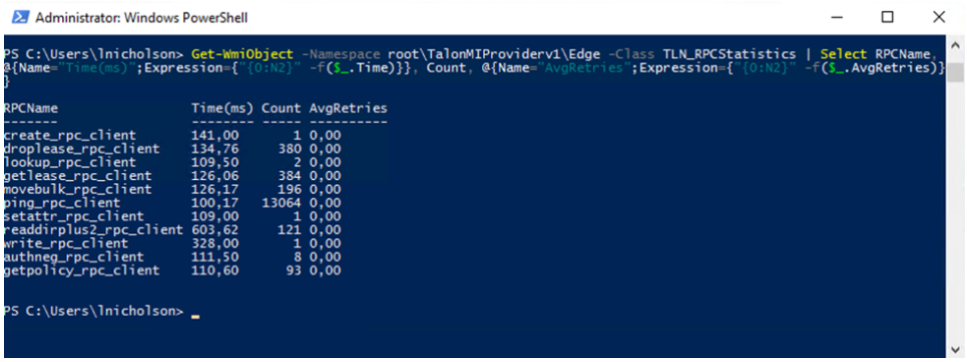
```
Get-WmiObject -Namespace root\TalonMIProviderv1\Core -Class TLN_RPCStatistics
| Select RPCName, @{Name="Time(ms)";Expression={"{0:N2}" -f($_.Time)}},
Count, @{Name="AvgRetries";Expression={"{0:N2}" -f($_.AvgRetries)}}
```

   Edge Command:

```
Get-WmiObject -Namespace root\TalonMIProviderv1\Edge -Class TLN_RPCStatistics
| Select RPCName, @{Name="Time(ms)";Expression={"{0:N2}" -f($_.Time)}},
Count, @{Name="AvgRetries";Expression={"{0:N2}" -f($_.AvgRetries)}}
```

   Edge Output:

© 2020 NetApp, Inc. All Rights Reserved.



Dirty Files

The command gives you the ability to view any files that are currently in the Dirty Files DB.

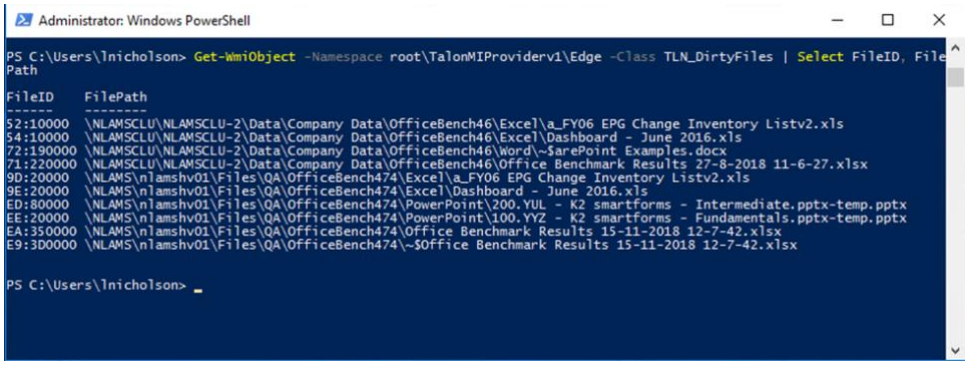
Display Dirty Files

Edge Command:

```
Get-WmiObject -Namespace root\TalonMIProviderv1\Edge -Class TLN_DirtyFiles | Select FileID, FilePath
```

Edge Output:

Figure 47)



Active Fetches

Provides you with the ability to check for any current Fetches within the GFC Fabric.

Display Active Fetches

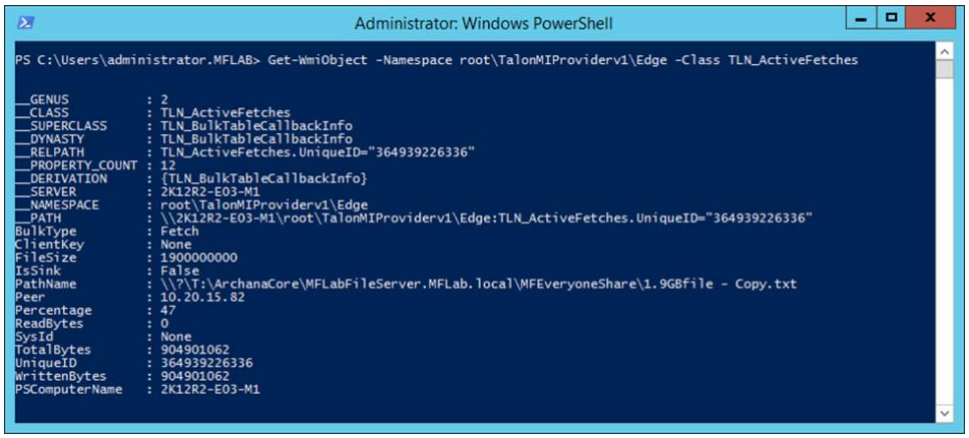
Edge Command:

```
Get-WmiObject -Namespace root\TalonMIProviderv1\Edge -Class TLN_ActiveFetches
```

Edge Output:

© 2020 NetApp, Inc. All Rights Reserved.

Figure 48)



Active Flushes

Provides you with the ability to check for any current Flushes within the GFC Fabric.

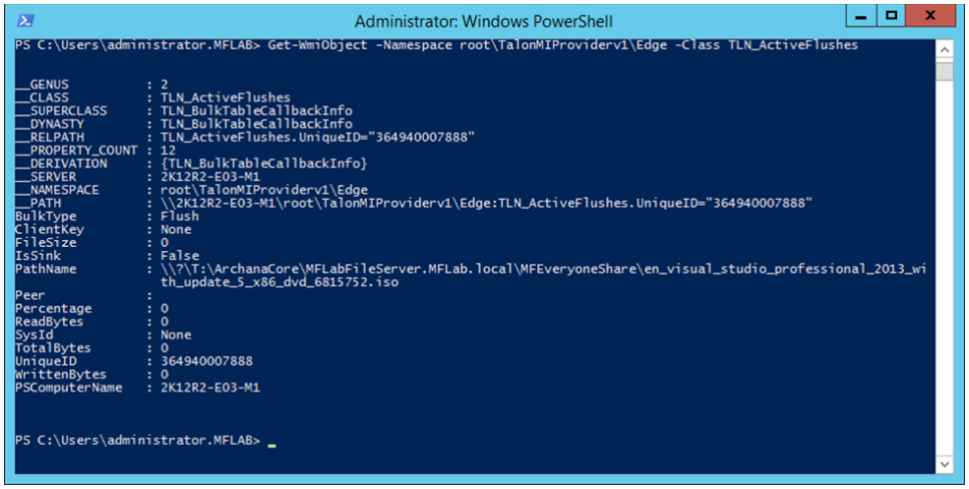
Display Active Flushes

Edge Command:

```
Get-WmiObject -Namespace root\TalonMIProviderv1\Edge -Class TLN_ActiveFlushes
```

Edge Output:

Figure 49)



© 2020 NetApp, Inc. All Rights Reserved.

§Appendix D: NetApp Global File Cache Event ID / Logging / 3rd Party Monitoring

NetApp Global File Cache Event IDs

NetApp Global File Cache (GFC) provides enhanced logging of system state, events and errors/warning associated with the solution deployment. The following events are logged in the Microsoft Windows Event Viewer as well as in the GFC log files as stored in

`C:\Program Files\TalonFAST\FASTDebuglogs\<folder on each Core or Edge instance>.`

Below Table 2 you can find the most common events to monitor, event ID, description and severity.

Table 2)

Event ID	Event	Description	Severity
262	Error on Connection to <IP address>	Indicator that network connectivity may have been briefly impacted between Edge and Core. The connections will re-establish automatically	Warning
274 (Core)	Connection from <Edge><EdgeIP> successfully established	Connections from Edge to the Core have been established successfully.	Information
274 (Edge)	Connections established and authenticate with <Core>	Connections between Edge and Core have been established successfully.	Information
280	From/To Datacenter (Gathered-Write)	Informational message that data is being read fetched from or flushed to the Datacenter. This will be visible from the Edge and from the Core	Information
285	Site key validated for all connections to <Core>. Transitioning to CONNECTED mode.	WAN disconnection resolved, Edge and Core are communicating as normal.	Information
287	Unable to get address for <core>: error 11001 (No such host is known)	Indicates a DNS error where Core cannot be resolved. 347 – Transitioning to DISRUPTED mode for <Core> Indicates a dropped or lost connecting to the Core. Potentially a WAN error or outage. This should be followed by ID 285.	Error
3328	Talon PrePopulation started at <Time> on <Date> with max_threads 15	Indicates the start time and date of a pre-population with the default thread count of 15.	Information
3329	Job is picked up for execution <BackendFS> (Edge)	Indicates a new Pre-population job has been picked up for execution on the Edge	Information
3329	Job has been completed <BackendFS> (Edge)	Indicates that a Pre-population job has started and completed	Information

© 2020 NetApp, Inc. All Rights Reserved.

282	Cache Cleaner process is initiated	Automated purging mechanism is engaged. Indicated cache has reached 85% capacity. May adjust D:\ accordingly if desired	

GFC Logging

GFC log files are stored in C:\Program Files \TalonFAST\FASTDebugLogs\

The Logs are rotated every 8 Hours or every 1MB, keeping total of 72 hours.

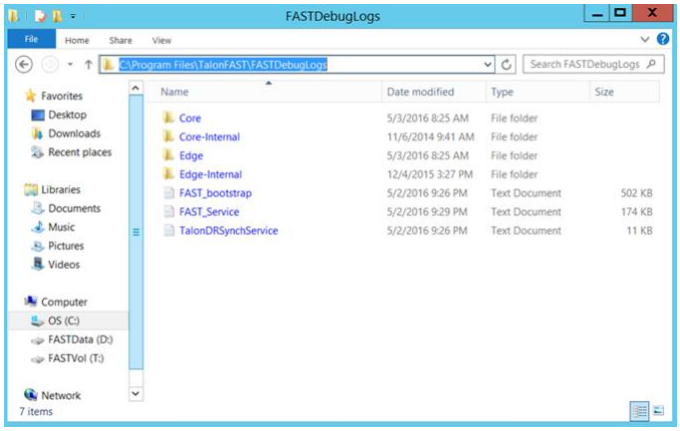
The “Core” and “Edge” directories house logs associated with Core and Edge activity:

- FAST File Transfer Logs
- FAST Messages Logs
- FAST Statistics Logs
- Pre-Population Logs

Core-Internal and Edge-Internal Directories

- These directories house Engineering level logs
- Logs in these directories may be requested from NetApp Support for troubleshooting purposes

Figure 50)



The content contained in the Log Files can be identified in the Table 3 below.

Table 3)

Log File	Description
File Transfer Log (Core and Edge) FAST_File_Transfer.txt	Logs individual file transfer activity Date and Path File Size / Bytes Transferred / Bytes Exchanged / Transfer Efficiency
FAST Statistics Log (Core) FAST_Stats.txt	Logs Server-Side Statistics File Statistics Compression / Differencing Efficiencies Current File Leases
FAST Statistics Log (Edge) FAST_Stats.txt	Logs Client-Side Statistics Connected Core information

© 2020 NetApp, Inc. All Rights Reserved.

	Compression / Differencing Efficiencies
Messages Log FAST_Messages.txt	Logs system messages / error conditions
Pre-Population Log (Edge only) Tapp.txt	Logs start and end times of pre-population jobs Displays individual files / folders transferred

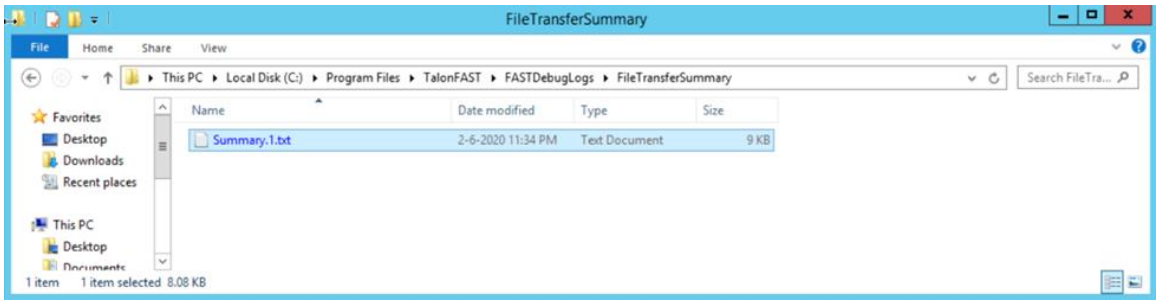
GFC File Transfer Summary Logging

Additional logging has been introduced to capture file activity, which can provide for optimized reporting purposes and analysis using any 3rd party log parsing tool.

The log file is automatically generated on the GFC core instance and can be found in the following location:

```
C:\Program Files\TalonFAST\FASTDebugLogs\FileTransferSummary\
```

Figure 51)



The log file contains a breakdown of the file type, direction (fetch / flush), backend file server hosting the source file storage, the backend file-share, the GFC edge instance that has been requesting the file(s), a count of the amount of files fetched or flushed over the WAN, the minimum and maximum file sizes, average file size and the average transfer efficiency. All statistics are aggregated in bytes traversing the WAN and

Figure 52)

FileType	Direction	Backend	Share	Edge	Count	MinSize	MaxSize	AvgSize	AvgTransEff
.xlsx	FLUSH	nlamshv01	Files	10.0.30.21	839	0	48654540	2227838.13	2367478.65
.docx	FLUSH	nlamshv01	Files	10.0.30.21	815	0	41921280	375460.55	397055.05
.doc	FLUSH	nlamshv01	Files	10.0.30.21	139	0	0	0	170.51
.tmp	FLUSH	nlamshv01	Files	10.0.30.21	118	0	3573766	206195.2	317879.6
.docx	FETCH	nlamshv01	Files	10.0.30.21	36	11549	731858	257751.86	1204.06
.DOC	FLUSH	nlamshv01	Files	10.0.30.21	50	0	0	0	173
.xls	FLUSH	nlamshv01	Files	10.0.30.21	101	55296	2642944	1361930.14	17246.64
.xls	FETCH	nlamshv01	Files	10.0.30.21	1	2100224	2100224	2100224	4189
.pptx	FLUSH	nlamshv01	Files	10.0.30.21	1010	0	3573772	175042.19	219181.81
.pptx	FETCH	nlamshv01	Files	10.0.30.21	64	408151	3573772	2945554.09	5840.5
.xlsx	FETCH	nlamshv01	Files	10.0.30.21	76	10211	824551	271537.66	613.11
.xlsx	FLUSH	nlamshv01	Files	192.168.1.210	645	0	185385075	13643343.84	13703453.72
.docx	FETCH	nlamshv01	Files	192.168.1.210	10	800020	6736830	2566284.7	2166806.2

GFC Processes / Services

GFC leverages different services and processes to establish and maintain the GFC Fabric and its associated GFC Core and GFC Edge instances. Some of these are dependent on other services and the TFAST.SYS file system kernel driver, which enables the GFC Virtual File Share and Intelligent File Cache on each GFC Edge instance.

The Table 4 below provides you with the details for each service and the functionality it provides.

© 2020 NetApp, Inc. All Rights Reserved.

Table 4)

Process/Service	Description
Tservice.exe (GFC Modules Service Monitor)	Job is to spawn Tum service in either Core, Edge or Hybrid mode Also spawns Tapp.exe and TFS.exe This is a Service
Tum.exe (GFC User Module)	Intelligent File Caching workhorse This is a process spawned on both GFC Core and Edge instance (Tum.exe –s & Tum.exe –c)
Tapp.exe (GFC Pre-Population)	Processed used for Pre-Population
Optimus.exe (GFC Configuration Console)	Configuration management software used when configuring an appliance This is a Process
LMCService.exe (GFC License Manager Client)	Used by GFC Servers to register with the license management server Spawns the Tservice.exe
LMSService.exe (GFC License Manager Server)	Used by GFC License management server Accepts the incoming client request for LMCService.exe

Where to Find Additional Information

To learn more about the information that is described in this document, review the following documents and/or websites:

- This video provides a general solution overview to admins and users as well as providing some GFC do's and don'ts.
  https://youtu.be/bH5T1KX79aM
- This video provides a general solution overview to admins and users as well as providing some GFC do's also provides a shortened general overview, basic do's and don'ts, and a focus on Autodesk Revit application best practices.
  https://youtu.be/avMMA_ltZy0

© 2020 NetApp, Inc. All Rights Reserved.

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

Copyright Information

Copyright © 2020 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.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, 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).

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.

© 2020 NetApp, Inc. All Rights Reserved.

Software Usage Limitations

You should be aware that the following additional limitations apply to your use of the GFC:

1. *Unless authorized explicitly in writing by NetApp, Customers who have initially licensed Talon FAST™ after March 9, 2020, are only authorized to run and install Talon FAST™ on the following backend products: NetApp's Cloud Volumes ONTAP® Software, NetApp's Cloud Volumes Service for Amazon Web Services, NetApp's Cloud Volumes Service for Google Cloud Platform, or Azure NetApp Files.*
2. *Provided it's released during the license term, Customers who have initially licensed Talon FAST™ after March 9, 2020, will, unless authorized explicitly in writing by NetApp, be required to upgrade to the next version of the Talon FAST™ Software (Global File Cache v. 1.0) when its released (tentatively Spring 2020).*
3. *Subject to the foregoing limitations, Customers which have been provided a license to Talon FAST™ at no charge are entitled to use that license for a period not to exceed 12 months from the date of initial software installation.*

© 2020 NetApp, Inc. All Rights Reserved.