EMC²

TECHNICAL NOTES

Configuring BranchCache V2 on VNX®

Technical Notes

P/N H10813
January 6, 2014

This technical note contains information on these topics:

Introduction

The trend today is for companies to have a centralized main office and several other geographical sites or branch offices. Data is centralized in the main office, and users at the branches retrieve data from the main office as required. Generally, branch offices are connected to the main office by using a slow and expensive WAN link. This has several drawbacks:

- High link utilization
- Poor application responsiveness
- Expensive WAN link bandwidth

BranchCache is a Microsoft® feature that is described as a wide area network (WAN) bandwidth optimization technology. It was first introduced in the Windows® 7 and Windows Server 2008 R2 operating systems, but has since been updated to include Windows 8 and Windows Server 2012 operating systems. When BranchCache is enabled, it creates a cache of the content from the file server locally within a branch office. A client from the same network can request the file and download it from the local cache instead of downloading it from the wide area network. BranchCache optimizes the local link utilization, increases the responsiveness of applications, and reduces the WAN bandwidth consumption.

Note: A write request goes directly to the file server in the main office.

Audience

The document is intended for VNX customers who have several geographical sites linked by WAN or slow networks and want to use Microsoft BranchCache to save bandwidth consumption and improve response time on those links.

Technical overview

Signature

The mechanism for reducing bandwidth is to generate a unique signature of a file that is approximately 1000 times smaller than the actual content. VNX divides the data into fixed 128KB segments. A hash algorithm is then run on the segments to generate the content signature. The hashed content includes both the hash of the data and the segment secret, which is used to derive an encryption key for data protection. This signature is provided instead of the file when the file is requested. The default hash algorithm used to generate this signature is SHA 256. The minimum file size that will generate a signature is 128KB by default. When the content is less than 128KB, data is directly retrieved from the VNX through the WAN.

Modes

Depending on the location of the cache, BranchCache can operate in either Hosted Cache mode or Distributed Cache mode. In both modes, VNX plays the role of the content server located in the main office where clients connect to retrieve files. Both modes are mutually exclusive. A client computer can be configured to use only a single caching mode at a time.

Hosted Cache mode

The Hosted Cache mode operates by deploying a server(s) that plays the role of cache in the branch office. This server stores the content that is downloaded by clients at the branch office and makes it available to the other clients at the same branch. If the content is not available on the Hosted Cache server, it is retrieved from the content server by using the WAN and then offered to the Hosted Cache server so that subsequent clients can benefit from it. Also, clients on different subnets in a multiple-subnet branch office would be able to access the server, unlike in Distributed Cache mode.

Figure 1 describes the document caching and retrieval process using Hosted Cache mode.

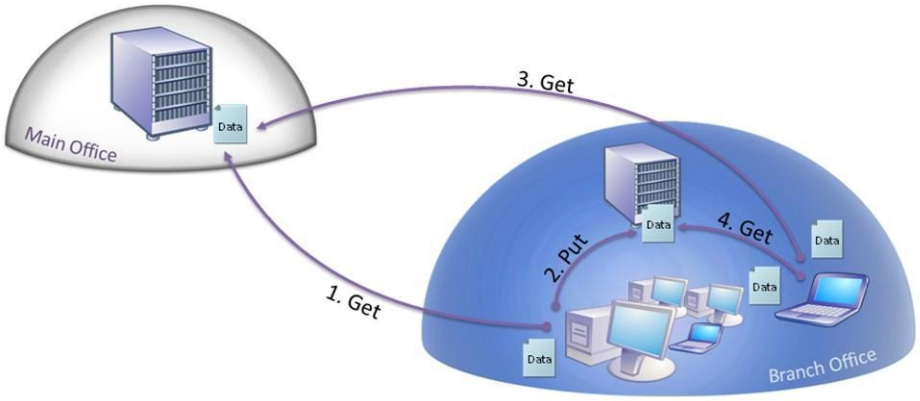


Figure 1: Hosted Cache mode

Hosted Cache mode uses the following process to cache and retrieve data:

1. A client connects to the content server and requests a file or part of a file.
    a. The content server authenticates and authorizes the client exactly as it would without using BranchCache. If successful, the content server returns the content signature over the same channel through which data would normally have been sent.
    b. The client uses this signature to search for the file in the Hosted Cache server. Because this is the first time any client has retrieved the file, it is not already cached on the Hosted Cache server. Therefore, the client retrieves the file directly from the content server.
2. The client establishes a Secure Socket Layer (SSL) connection with the Hosted Cache server and offers the content identifier over this encrypted channel.
    a. The Hosted Cache server connects to the client and retrieves the set of data that it has not cached.
3. A second client requests the same file from the content server. The content server authorizes the user and returns the content signature.
4. The client uses this signature to request the data from the Hosted Cache server. The Hosted Cache server encrypts the data and sends it to the client. (The data is encrypted by using a symmetric key contained in the signature and derived from the content data).

a. The client decrypts the data, computes the signature of the data received from the Hosted Cache server, and ensures that the data is identical to the signature that was sent by the content server. This ensures that the content has not been modified.

Distributed Cache mode

For branch offices with less than 50 users, configure BranchCache in Distributed Cache mode. In this mode, local clients at the branch office keep a copy of the content and make it available to other clients that request the same file. This eliminates the need to have a dedicated server in the branch office. However, unlike Hosted Cache mode, this configuration works across a single subnet only. The content must be retrieved once per subnet in the branch office through the WAN. In addition, the clients that disconnect from the network are not able to provide content to requesting clients.

Figure 2 describes the caching and retrieval process through the Distributed Cache mode.

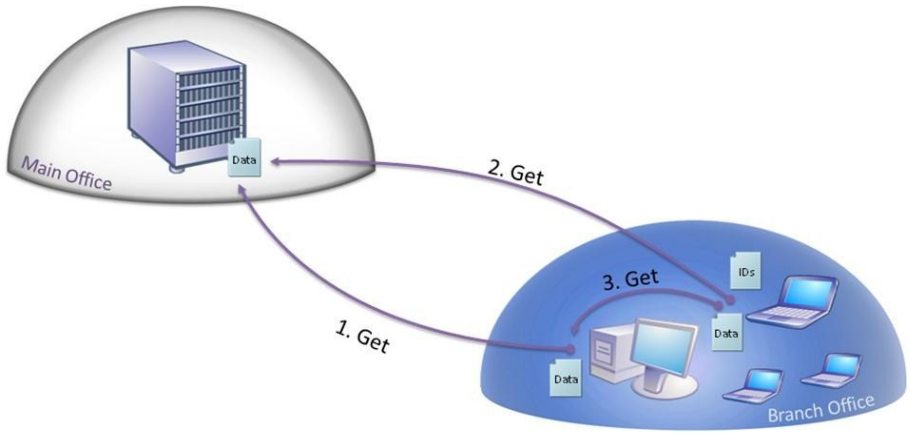


Figure 2: Distributed Cache mode

Distributed Cache mode uses the following process to cache and retrieve data:

1. A client connects to the content server and requests a file or part of a file.
   a. The content server authenticates and authorizes the client exactly as it would without using BranchCache. If successful, the content server returns the content signature over the same

channel through which data would normally have been sent.

b. The client uses this signature to search for the file on the local network. Because this is the first time any client has attempted to retrieve the file, it is not cached already on the local network. Therefore, the client retrieves the file directly from the content server and caches it.

2. A second client requests the same file from the content server. The content server authenticates and authorizes the client exactly as it would without using BranchCache. If successful, it returns the content signature over the same channel through which data would normally have been sent.

   a. The second client sends a request on the local network for the required file by using the Web Services Discovery (WS-Discovery) multicast protocol.

3. The client that previously cached the file sends the file to the requesting client. The data is encrypted by using a symmetric key contained in the signature and derived from the content data.

   a. The client decrypts the data, computes the signature of the data received from the first client, and ensures that the data is identical to the signature provided by the content server. This ensures that the content has not been modified.

Configuring BranchCache

System requirements

- **Client Computers** – Certain editions of Windows operating systems can act as BranchCache clients. The following versions are supported:
    - Windows 8 Enterprise
    - Windows 7 Enterprise
    - Windows 7 Ultimate
- **Content Servers** – Most Windows servers have BranchCache content server functionality. The following versions can be used as BranchCache content servers:
    - The Windows Server 2012 family of operating systems
    - The Windows Server 2008 R2 family of operating systems, with the following exceptions:
        - Windows Server 2008 R2 Enterprise with Hyper-V
        - Windows Server 2008 R2 Datacenter with Hyper-V
- **Hosted Cache Servers** – Several editions of Windows servers have BranchCache hosted cache server functionality. The following versions can be used as BranchCache hosted cache servers:
    - The Windows Server 2012 family of operating systems
    - Windows Server 2008 R2 Enterprise
    - Windows Server 2008 R2 Enterprise with Hyper-V
    - Windows Server 2008 R2 Enterprise Server Core Installation
    - Windows Server 2008 R2 Enterprise Server Core Installation with Hyper-V

  - Windows Server 2008 R2 for Itanium-Based Systems
  - Windows Server 2008 R2 Datacenter
  - Windows Server 2008 R2 Datacenter with Hyper-V
  - Windows Server 2008 R2 Datacenter Server Core Installation with Hyper-V

- EMC VNX Operating Environment (OE) for File version 7.1 or later
- The clients should be located at the branch office and the VNX in the main office
- Domain and Enterprise Admin privileges (Hosted Cache mode only)

Signature

Hash generation is disabled by default. It can be enabled through a Group Policy Object (GPO) or by editing a Registry key on the CIFS server.

> Note: The Registry setting is overridden by the domain GPO setting, and any changes will take effect immediately.

The location of the GPO is:

Computer Configuration\Policies\Administrative Templates\Network\Lanman Server\Hash Publication for BranchCache

The location of the Registry key on the CIFS server is:

HKEY_LOCAL_MACHINE\Software\EMC\SmbHash\Hash Publication

This is an integer with three possible values:

0: Allow hash publication only for shared folders with the 'HASH' flag set. The 'HASH' flag can be set on the CIFS share by using the `server_export` command.

1: Disallow hash publication on all shared folders. No SMB Hash Files can be generated. This is the default setting.

2: Allow hash publication for all shared folders.

The next section explains the use of the CIFS server Registry key to enable hash publication.

Enable Hash Publication

Hash generation is disabled by default and can be enabled by editing a Registry key on the CIFS server or by a Group Policy Object (GPO).

1. On a Windows 8 system, right click **Start > Run >** [type regedit] **> Enter.**
2. Go to **File > Connect Network Registry >** [type name of CIFS server you are using] **> Check Names > OK.**
3. Under connected CIFS server go to: HKEY_LOCAL_MACHINE/Software/EMC/SmbHash.
4. Verify that **Enable** has a data value of **1**.
5. Change **Hash Publication** to a value of **2**. (This allows hash publication for all shares. A value of **0** only allows shares with a hash flag set for hash publication. A value of **1** disallows hash publication on all shared folders.)

Enable BranchCache on Data Mover

1. Enable BranchCache service.
   a. SSH to your Control Station.
   b. Log in as nasadmin.
   c. Type su.
   d. Enter root password.
   e. Type `server_cifs server_2 –smbhash –service enable`

```
[nasadmin@P23-0436-17111 ~]$ server_cifs server_2 -smbhash -service enable
server_2 :
smbHash service started.
smbhash service is enabled.
```

2. Enable BranchCache auditing. This allows you to see audit information in the event logs from your Windows system.
   a. Type `server_cifs server_2 –smbhash –audit enable`

```
[nasadmin@P23-0436-17111 ~]$ server_cifs server_2 -smbhash -audit enable
server_2 :
smbhash Windows events is enabled.
```

3. Restart CIFS service on the Data Mover. This can be done either through the SSH session or Unisphere.

For SSH:

a. Type `server_setup server_2 –P cifs –o stop`

b. Type `server_setup server_2 –P cifs –o start`

```
[nasadmin@P23-0436-17111 ~]$ server_setup server_2 -P cifs -o stop
server_2 : done
[nasadmin@P23-0436-17111 ~]$ server_setup server_2 -P cifs -o start
server_2 : done
```

For Unisphere:

a. Click the **Storage** tab.

b. Under **File Storage** in right column, click **Configure CIFS.**

c. Uncheck **CIFS Service Started** checkbox and click **Apply**. Then check the same box and click **Apply** again.

4. Confirm BranchCache service was successfully enabled.

Type `server_cifs server_2 –smbhash –info`

```
[nasadmin@P23-0436-17111 ~]$ server_cifs server_2 -smbhash -info
server_2 :
Current smbhash parameters:
---------------------------
Enabled             : Yes
Started             : Yes
```

Configuring Hosted Cache mode

For Windows Server 2012:

1. In Windows Server 2012, start Windows PowerShell as an administrator.

a. Right-click **Start > Search.**

b. Type **Windows PowerShell.**

c. Right-click **Windows PowerShell.**

d. Click **Run as administrator**.

Note: Do not use Windows **PowerShell (x86)**.

2. Install BranchCache on the server.

Type `Install-WindowsFeature BranchCache –IncludeManagementTools`

3. Configure the computer as a hosted cache server.

Type `Enable-BCHostedServer –RegisterSCP`

4. Verify that the service mode is set to **Hosted Cache Server** and the current status set to **Running**.

Type `netsh branchcache show status all`

```
PS C:\Users\administrator.PRODCSE> Install-WindowsFeature BranchCache -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {BranchCache}


PS C:\Users\administrator.PRODCSE> Enable-BCHostedSErver -RegisterSCP
PS C:\Users\administrator.PRODCSE> netsh branchcache show status all


BranchCache Service Status:
--------------------------------------------------------------------------------
Service Mode          = Hosted Cache Server
Client Authentication = Domain Authentication
Current Status        = Running
Service Start Type    = Automatic
This machine is currently configured as a hosted cache server.
```

For a Windows 8 client:

1. In a Windows 8 client, start Windows PowerShell as an administrator.
   a. Right click **Start > Search**.
   b. Type **Windows PowerShell**.
   c. Right-click **Windows PowerShell.**
   d. Click **Run as administrator**.

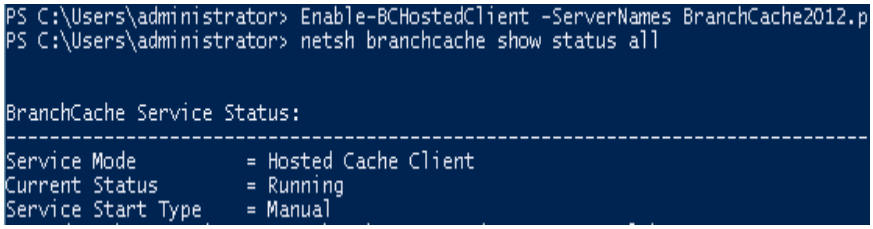
   Note: Do not use **Windows PowerShell (x86)**

2. Enable the computer as a hosted client to the configured hosted cache server.

Type `Enable-BCHostedClient –ServerNames <FQDN of your Win2012 server>`

3. Verify that the service mode set to **Hosted Cache Client** and current status is set to **Running**.

Type `netsh branchcache show status all`



Configuring Distributed Cache mode

For a Windows 8 client:

1. Start the command prompt window as an administrator.
   a. Right click Start.
   b. Click Command Prompt (Admin).
2. Enable BranchCache for the client.

Type `netsh branchcache set service mode=DISTRIBUTED`

Note: This can also be done through a group policy object to enable many clients quickly.

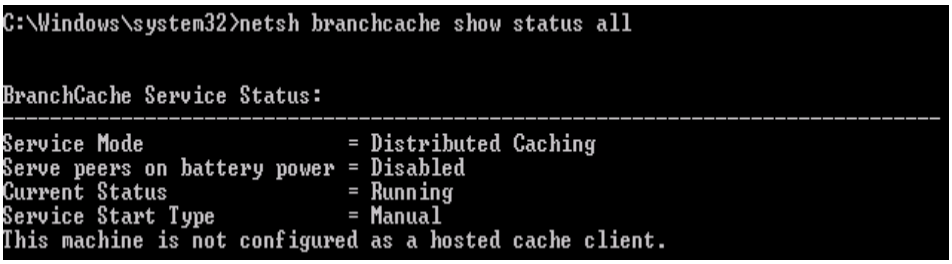
3. Set maximum latency the client should see before using BranchCache.

Type `netsh branchcache smb set latency latency=<latency in ms>`

Note: The default is 80 ms. If you want to ensure BranchCache will be used every time, set the latency to 0 ms.

4. Verify BranchCache is set for **Distributed Caching** and **Current Status** is **Running**.

Type `netsh branchcache show status all`



Viewing BranchCache information

SMB Hash statistics

VNX keeps a track of BranchCache statistics, such as hits or misses, number of hashes generated, and hash generation times and sizes. This information can be used for troubleshooting when hash generation issues on VNX are suspected. BranchCache configuration information is displayed here also. To view this information, run the following command:

```
server_cifs server_2 -smbhash –info
```

Example output:

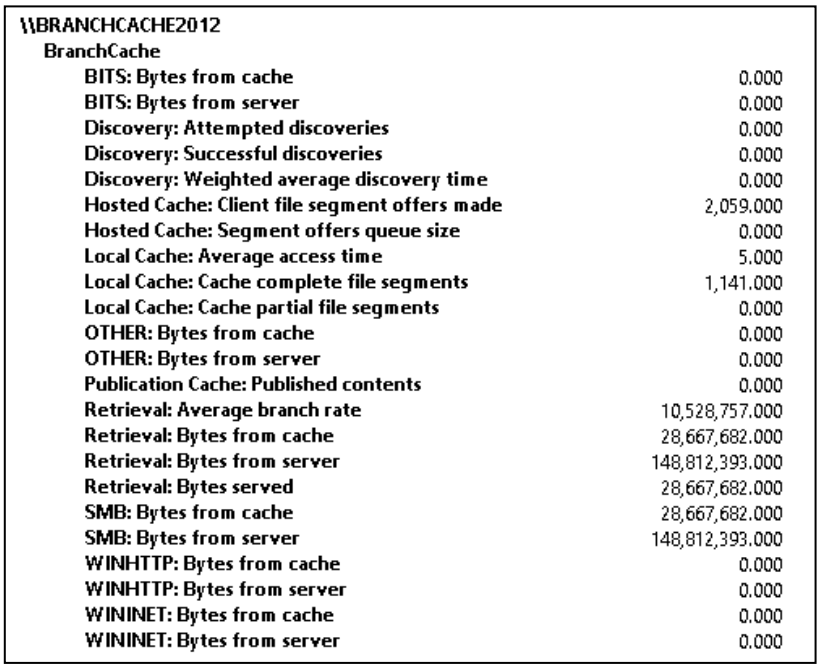
```
[nasadmin@P23-0436-17111 ~]$ server_cifs server_2 -smbhash -info
server_2 :
Current smbhash parameters:
---------------------------
Enabled             : Yes
Started             : Yes
RunningThreads      : 3
NumberOfThreads     : 3
HashPublication     : ALL
HashSupportedVersion: Undefined
HashAlgo (V1)       : SHA_256
BlockSize (V1)      : 64 kB
BlocksPerSegmt (V1) : 512
SegmentSize (V2)    : 128 kB
TaskQueueSize       : 32
ExclusionFilter     : None
MinRequiredAgeFile  : 60 sec
NextTaskID          : 20
CleanupMinTime      : 300 s
CleanupDeltaDBSize  : 10%
CleanupDeltaFsSize  : 10%
CleanupFsSizeDivider: 100
Audit               : All (7)

No running smbhash tasks.

SmbHash statistics:
-------------------
IOCTL (any hash version)                : 148 hits / 19 misses / 3401 kb of ha
sh transferred
                        hash version 1  : 0 hits / 0 misses / 0 kb of hash tra
nsferred
                        hash version 2  : 148 hits / 19 misses / 3401 kb of ha
sh transferred
number of generated hash files          : 19 success / 0 failures / 0 filtered
size of generated hash files (all/max/min): 404 kb / 53 kb / 322 b
time to generate hash files (avg/max/min) : 312 ms / 815 ms / 3 ms
```

BranchCache performance statistics

BranchCache performance information can be viewed directly from Windows with the Performance Monitor tool. The performance statistics shown here apply only to the individual client. This information is useful when only a particular client is acting abnormally. To view this information, follow these steps:

1. On your Windows client or Windows server, open the Performance Monitor tool.
   a. Right click **Start**.
   b. Click **Run.**
   c. Type "perfmon".
   d. Click **OK**.
2. Clear processor information.
   a. Click **Performance Monitor** under the **Monitoring Tools** folder.
   b. Click the **Change Graph Type** drop-down button.
   c. Select **Report**.
   d. Click **Processor Information.**
   e. Press the **Delete** key. (The report should now be blank).
3. Add BranchCache performance information.
   a. Click the Add button (green plus sign).
   b. Select **BranchCache** from the list.
   c. Click Add.
   d. Click OK.

Example output:



\\BRANCHCACHE2012	
BranchCache	
BITS: Bytes from cache	0.000
BITS: Bytes from server	0.000
Discovery: Attempted discoveries	0.000
Discovery: Successful discoveries	0.000
Discovery: Weighted average discovery time	0.000
Hosted Cache: Client file segment offers made	2,059.000
Hosted Cache: Segment offers queue size	0.000
Local Cache: Average access time	5.000
Local Cache: Cache complete file segments	1,141.000
Local Cache: Cache partial file segments	0.000
OTHER: Bytes from cache	0.000
OTHER: Bytes from server	0.000
Publication Cache: Published contents	0.000
Retrieval: Average branch rate	10,528,757.000
Retrieval: Bytes from cache	28,667,682.000
Retrieval: Bytes from server	148,812,393.000
Retrieval: Bytes served	28,667,682.000
SMB: Bytes from cache	28,667,682.000
SMB: Bytes from server	148,812,393.000
WINHTTP: Bytes from cache	0.000
WINHTTP: Bytes from server	0.000
WININET: Bytes from cache	0.000
WININET: Bytes from server	0.000

Figure 3: BranchCache performance information

BranchCache auditing logs

BranchCache auditing can be enabled, which captures BranchCache events to a log on the CIFS Server. This information can be used to view BranchCache historical events.

Note: This is different from CIFS auditing. This feature is disabled by default.

The Configuring BranchCache section provides more information on how to enable auditing. Once auditing has been enabled, you can view the logs by doing the following:

1. Open Computer Management tool.
   a. In a Windows client or server, right click **Start**.
   b. Click **Computer Management**.
2. Connect to CIFS server.

a. Right-click **Computer Management (Local)**.

b. Click **Connect to another computer**.

c. Click **Browse**.

d. Type the CIFS server name.

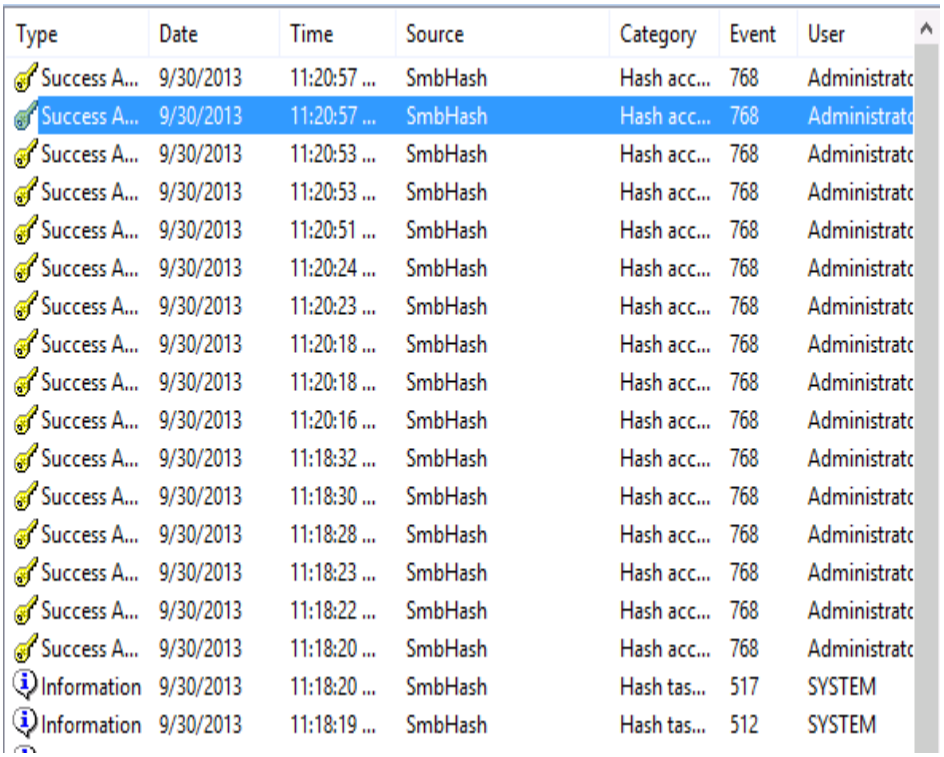
e. Click **Check Names**.

f. Click **OK**.

3. Navigate to the activity log.

Go to **System Tools > Event Viewer > Classic Event Viewer > Global Logs > SmbHash**.

Example output:



Type	Date	Time	Source	Category	Event	User
Success A...	9/30/2013	11:20:57 ...	SmbHash	Hash acc...	768	Administrato
Success A...	9/30/2013	11:20:57 ...	SmbHash	Hash acc...	768	Administrato
Success A...	9/30/2013	11:20:53 ...	SmbHash	Hash acc...	768	Administrato
Success A...	9/30/2013	11:20:53 ...	SmbHash	Hash acc...	768	Administrato
Success A...	9/30/2013	11:20:51 ...	SmbHash	Hash acc...	768	Administrato
Success A...	9/30/2013	11:20:24 ...	SmbHash	Hash acc...	768	Administrato
Success A...	9/30/2013	11:20:23 ...	SmbHash	Hash acc...	768	Administrato
Success A...	9/30/2013	11:20:18 ...	SmbHash	Hash acc...	768	Administrato
Success A...	9/30/2013	11:20:18 ...	SmbHash	Hash acc...	768	Administrato
Success A...	9/30/2013	11:20:16 ...	SmbHash	Hash acc...	768	Administrato
Success A...	9/30/2013	11:18:32 ...	SmbHash	Hash acc...	768	Administrato
Success A...	9/30/2013	11:18:30 ...	SmbHash	Hash acc...	768	Administrato
Success A...	9/30/2013	11:18:28 ...	SmbHash	Hash acc...	768	Administrato
Success A...	9/30/2013	11:18:23 ...	SmbHash	Hash acc...	768	Administrato
Success A...	9/30/2013	11:18:22 ...	SmbHash	Hash acc...	768	Administrato
Success A...	9/30/2013	11:18:20 ...	SmbHash	Hash acc...	768	Administrato
Information	9/30/2013	11:18:20 ...	SmbHash	Hash tas...	517	SYSTEM
Information	9/30/2013	11:18:19 ...	SmbHash	Hash tas...	512	SYSTEM

Use cases

Use Case 1:

Company A, a marketing company had a primary data center and headquarters in Chicago. The storage arrays hosted high-definition images, videos, and sound clips that were accessed by 500 users daily. The company recently opened two branch offices with 100 users each in New York and Los Angeles. Users from the branch offices often had to connect to the Chicago data center to retrieve large files. Users complained that the connection had always been slow and impacted their work. Management was concerned about missing important deadlines due to the performance issues.

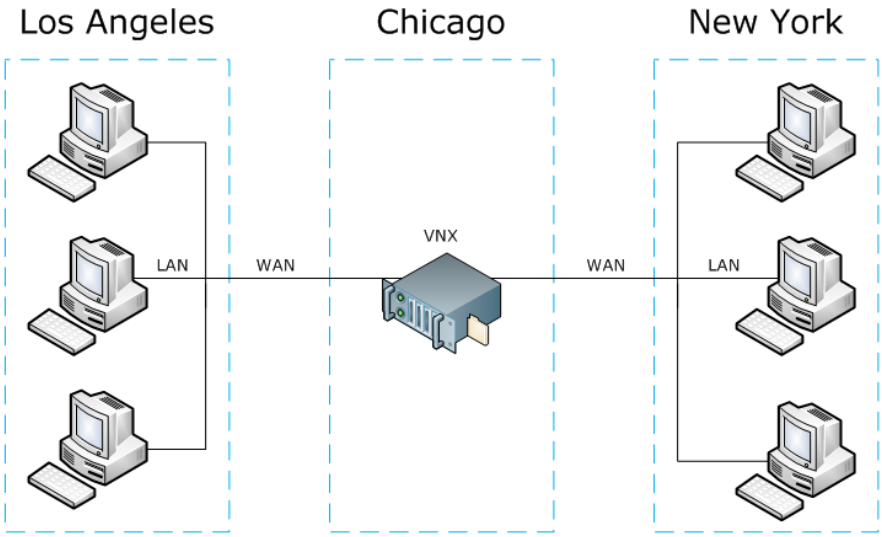


Figure 4: BranchCache enabled on VNX—Company A

Company A installed expensive dedicated WAN links, but performance was still poor due to congestion on the WAN. The company wanted a solution that would improve performance and reduce WAN link utilization. The IT team decided to try BranchCache because they already had all the requirements in place. The storage administrator enabled BranchCache on the VNX system to create a Content Server. The system administrators configured a server to act as the Hosted Cache server and enabled the BranchCache service on the clients at the branch offices.

Figure 5 shows BranchCache enabled on VNX at the Chicago office.

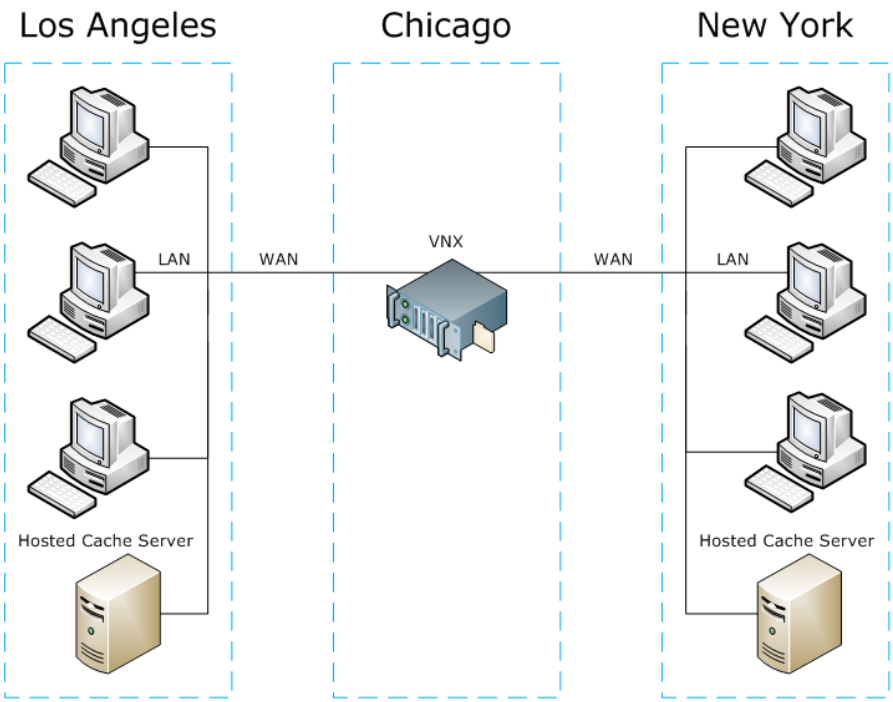


Figure 5: BranchCache using the Hosted Cache mode

The system administrators tested this solution by copying a file from the VNX system to a client at the New York office and confirmed that the performance was still slow. This was due to the file not being available on the Hosted Cache server because this was the first time that the file was requested. They copied the same file from the VNX system to another client at the same branch and noticed a significant improvement in performance. In the following days, they noticed that the WAN link utilization had started to gradually drop as more and more files became available at the Hosted Cache servers. Figure 6 shows BranchCache using the Hosted Cache mode.

By implementing BranchCache, Company A was able to successfully improve performance and reduce WAN link utilization. Once the commonly used files were available on the Hosted Cache servers, users reported a significant increase in performance. The reduction in traffic on the WAN link also resolved their congestion issues, so it also increased performance on files that needed to be transferred over the WAN.

Use case 2:

Company B had their headquarters located in Dallas, along with a sales office in San Francisco. The development, marketing, and support teams, totaling 100 users, are in the main office. Twenty-five sales representatives work in the branch office. The data center acted as a central repository for the entire company. The remote sales team routinely connected to the main office to retrieve content that was developed by the marketing team located in the main office. However, the WAN link was very slow. Users at the branch office often transferred files to each other using USB flash drives instead of going through the WAN. They could not justify setting up another data center at the branch office due to the size of the office, so they wanted another solution.

The administrators enabled BranchCache on VNX and BranchCache Distributed mode on all clients at the branch office. No other changes were made to the environment.

Figure 7 describes the BranchCache configuration for Company B.

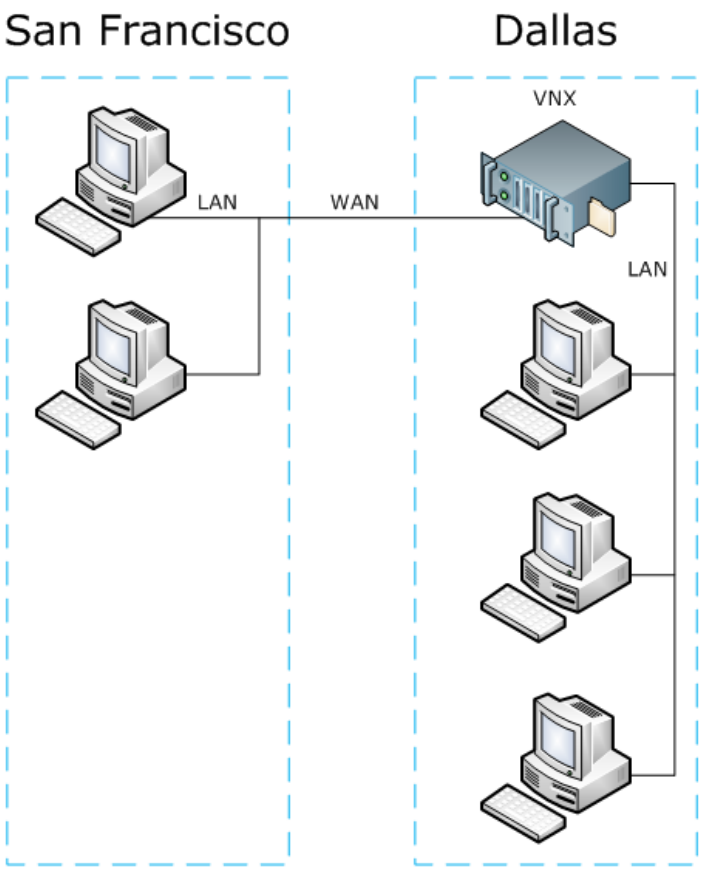


Figure 6: BranchCache for VNX—Company B

Users at the branch office can now go directly to the main office and transfer files from the content server. They now see a performance improvement compared to copying files through USB when the content is cached. When the content has not been cached, there is no difference in performance. Company B reported that BranchCache makes transferring files easier because they no longer need to copy data on to USB drives and pass it around.

Conclusion

As companies expand and start to place remote sites away from their headquarters, solutions are needed to ensure data can be transferred between offices which generally means use of expensive and limited bandwidth WAN links. As more files get requested from the main office by branch offices, these WAN links get overloaded resulting in slow application response time and frustrated employees. This is why BranchCache is an attractive solution due to the benefits it has including improved performance, reduced costs, and reduced WAN link utilization. Also, BranchCache is easy to set up because most users are likely to have all the requirements and infrastructure in place to support it. VNX assists BranchCache by acting as a content server that generates and manages signatures.

References

VNX

- BranchCache section - *Configuring and Managing CIFS on VNX*
  - EMC Online Support https://support.emc.com/

Windows

- BranchCache Overview
  - http://technet.microsoft.com/en-us/library/dd637832(v=ws.10).aspx
- BranchCache Deployment Guide for Windows Server 2008 R2 and Windows 7
  - http://www.microsoft.com/download/en/details.aspx?id=19558
- BranchCache for Windows Server 2008 R2
  - http://technet.microsoft.com/en-us/library/dd996634(v=ws.10)
- BranchCache Early Adopter's Guide
  - http://technet.microsoft.com/en-us/library/dd637762(v=ws.10)

Copyright © 2014 EMC Corporation. All Rights Reserved. Published in the USA.

Published January 2014

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

EMC2, EMC, and the EMC logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries. All other trademarks used herein are the property of their respective owners.

For the most up-to-date regulatory document for your product line, go to the technical documentation and advisories section on the EMC online support website.