What's New in IBM i NetServer Security and Management

Charles Emig
IBM i Development

emig@us.ibm.com

A Quick Recap of IBM i NetServer History

IBM i

- Added to the system in V4R2M0 (1996)
  - SMB1 in open internal LANs
  - NetBIOS over TCP/IP
- Added support to re-enable users disabled by too many bad connection attempts in V5R1M0 (2000)
- Updated to support SMB2 in V7R3M0 (2014)
  - Stronger authentication
  - Request chaining
- Updated to support SMB 3.0 in V7R4M0 (2018)
  - Encrypted sessions and share connections

Recent Windows 11 Experiences

IBM i

Windows 11 has become a continuous release product

- Like older Service Pack levels, but potentially more user impact

The recent 24H2 update made a change to more strictly enforce file name validation

Windows file system naming rules

> Use any character in the current code page for a name, including Unicode characters and characters in the extended character set (128–255), except for:
>
> The following reserved characters:
>
> < (less than)
> > (greater than)
> : (colon)
> " (double quote)
> / (forward slash)
> \ (backslash)
> | (vertical bar or pipe)
> ? (question mark)
> * (asterisk)

Some customers have files with invalid names that were created through application use of file system APIs

Recent Windows 11 Experiences

IBM i

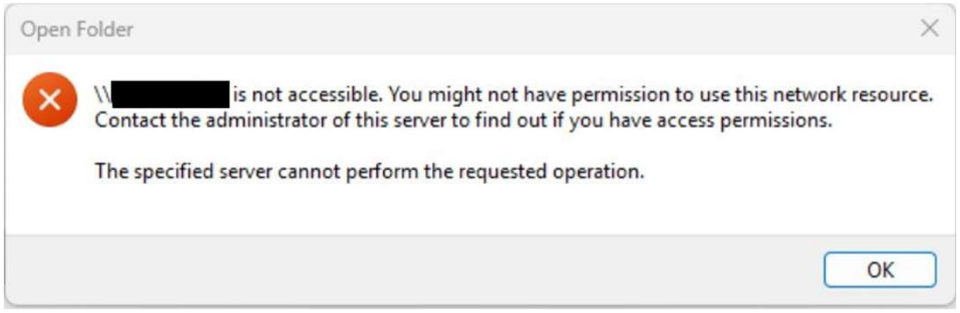
User impact

Pre-24H2

Objects with bad names may have been silently ignored by the client

With 24H2

Sudden inability to view specific shared directories after installing Windows 11 24H2



Recent Windows 11 Experiences

IBM i

[Finding and Renaming or Removing Invalidly Named Files from the Integrated File System]

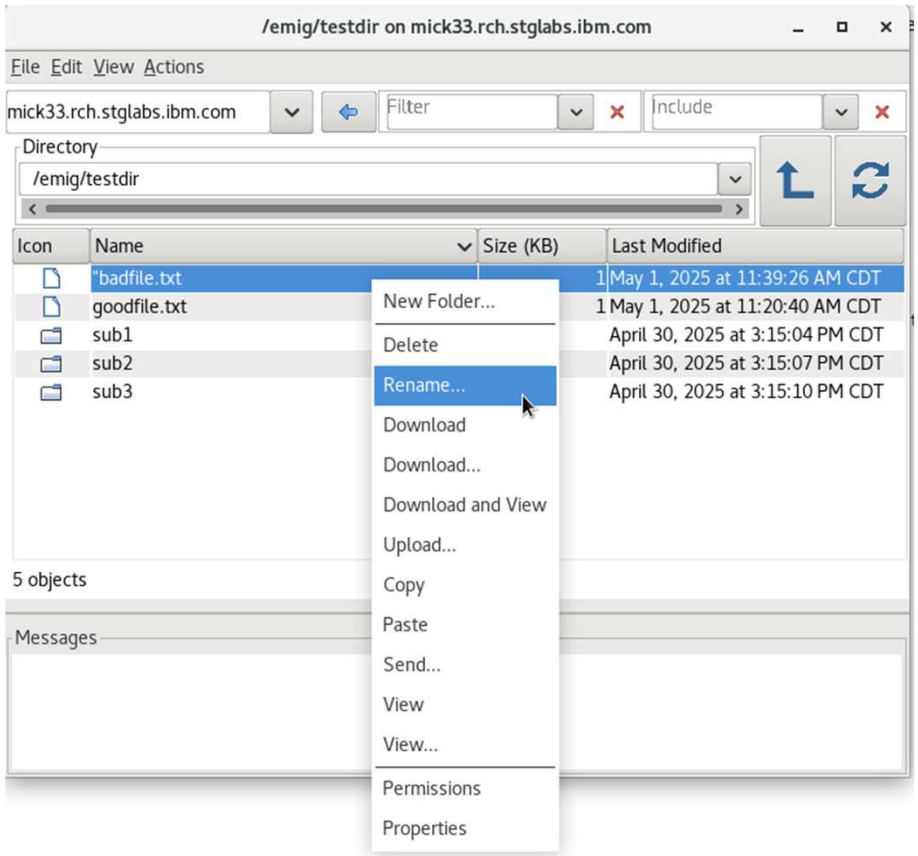
The following query can be used in Run SQL Scripts to find links that contain any of these characters except the forward slash (which is the default path delimiter character on IBM i so it is part of every path name). This query might take a very long time to complete:

```
SELECT PATH_NAME
  FROM TABLE (
       QSYS2.IFS_OBJECT_STATISTICS(
         START_PATH_NAME => '/', OMIT_LIST => '/QSYS.LIB /QNTC /QFILESVR.400', SUBTREE_DIRECTORIES => 'YES')
    )
  WHERE PATH_NAME LIKE '%\%'
     OR PATH_NAME LIKE '%<%'
     OR PATH_NAME LIKE '%>%'
     OR PATH_NAME LIKE '%|%'
     OR PATH_NAME LIKE '%*%'
     OR PATH_NAME LIKE '%:%'
     OR PATH_NAME LIKE '%?%';
```

The START_PATH_NAME can be set to the share path or even a sub-path if the problem share or path or is known.

Fixing Bad Names

The easiest way to fix bad names is to rename the object in the Integrated File System window in Access Client Solutions



Authorization List Restrictions (added in IBM i 7.5)

IBM i

What do they do?

- Authorization lists assigned to either the server or specific shares add an extra layer of restrictions to how users can access the resource
- They can be used to selectively choose which users can use NetServer
- They can be used to force some users to only have read-only access while others can still have write access if they have native write authority to the objects

What do they not do?

- Authorization list checks include user profile *ALLOBJ authority. Administrative users cannot be blocked and maintain full access.
- Authorization list authority cannot grant user authority to shared objects. Native permissions are still used to determine access and read-only shares will always be read-only. The most restrictive permission determines the level of access for a user.

When specifying an authorization list for the server:

- If a user is given at least *USE authority to the authorization list, that user will be allowed to access the server.
- If the user has less than *USE authority to the authorization list, the user will be denied access to the server, and a VP (Network) audit record entry type A (Authorization list (AUTL) permission failure) will be created.

When specifying an authorization list for a share:

- If a user is given *CHANGE or greater authority to the authorization list, that user will be allowed read/write access to the share.
- If a user is given *USE authority to the authorization list, that user will be allowed read only access the share.
- If the user has less than *USE authority to the authorization list, the user will be denied access to the share, and a VP (Network) audit record of entry type A (Authorization list (AUTL) permission failure) will be created.

Group authority checking was recently added via PTFs: MJ04704 and SJ04703

New Sharing Authority Requirement

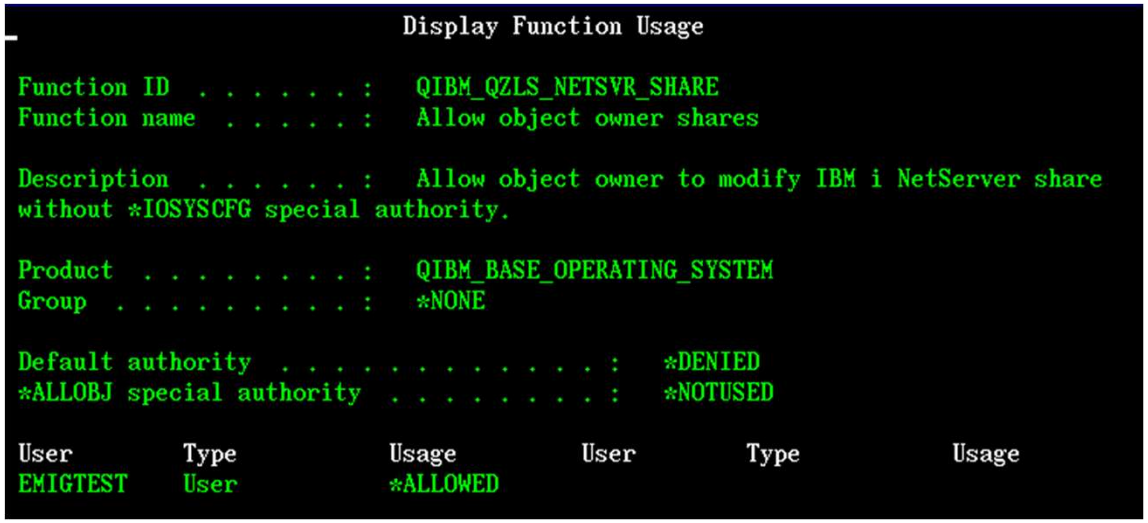
IBM i

Pre-7.6

- Owners of objects could share create a NetServer share even if that user didn't have *IOSYSCFG special authority
- Administrators had no native system control over preventing sharing by object owners

Now in 7.6

- Sharing requires *IOSYSCFG special authority by default for all objects. This restricts the ability to open new network access to the file system to administrative profiles designated to make changes to networking interfaces.
- A new function usage (QIBM_QZLS_NETSVR_SHARE) has been added that can selectively allow object owners to be granted sharing privileges.
- *ALLOBJ is not used when checking function usage. Access needs to be explicitly granted for non-*IOSYSCFG profiles.

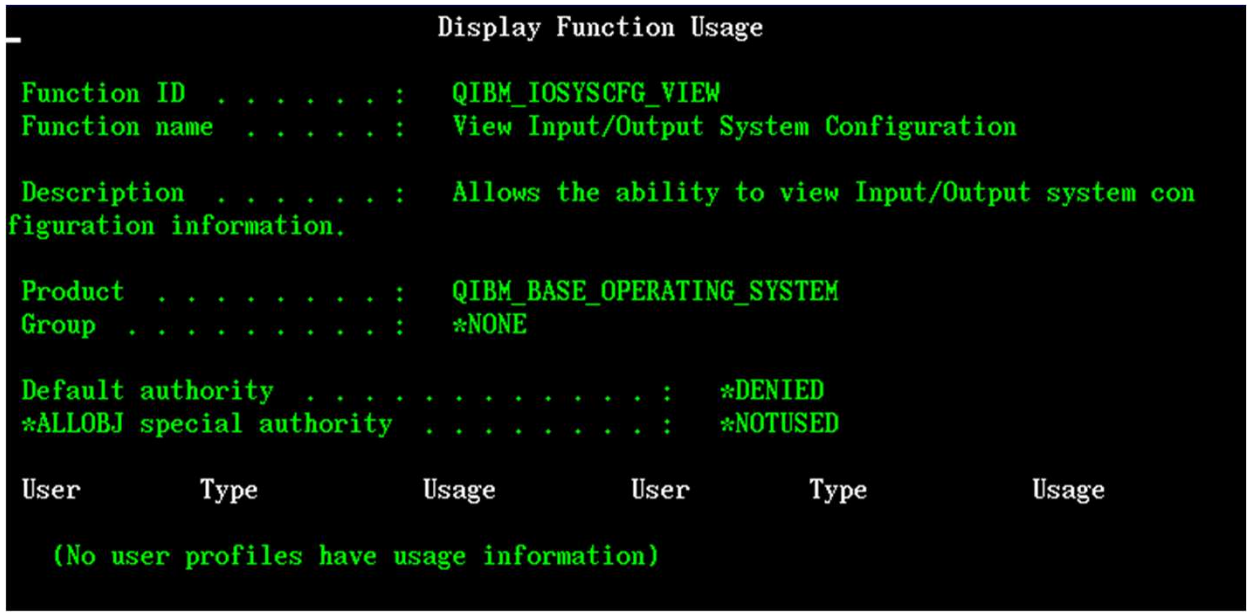


QIBM_IOSYSCFG_VIEW Function Usage

IBM i

Now in 7.6

- Viewing NetServer configuration information is now restricted to profiles with *IOSYSCFG special authority or profiles granted access to the QIBM_IOSYSCFG_VIEW function usage.
- This is a system-wide function usage created to improve security by restricting access to network configuration information to those who can change it or those explicitly granted authority to view the configuration.
- NetServer checks the function usage on the QZLSOLST and QZLSLSTI APIs used to view the server and share configuration.



Share Timestamps (added in IBM i 7.6)

IBM i

Each NetServer share has a set of create, update, and last accessed timestamps in IBM i 7.6. Times are currently only viewable through the QZLSLSTI and QZLSOLST APIs or in GO NETS. Navigator and SQL service support will be added later.

This is a new share that has never been accessed.

```
                        Display NetServer File Share

Share name . . . . . :  EMIG
Permissions  . . . . . :  *RW
Authorization list . . . :  *NONE
Require encryption . . . :  *NO
Maximum users  . . . . . :  *NOMAX
Current users  . . . . . :  0
Text 'description' . . . :  Chuck Emig user share
Path . . . . . :  /emig



Creation date/time . . . :  05/01/25 2:09:42 PM
Last change date/time  . :  05/01/25 2:09:42 PM
Last access date/time  . :  Not available
Text converting CCSID  . :  *NONE
Text converting  . . . . :  *NONE
Number of extensions . . :  0
Extension  . . . . . :
```

Shares migrated from a prior release may not have create or change times

Share Timestamps (added in IBM i 7.6)

IBM i

After the share has been accessed

```
                        Display NetServer File Share

Share name . . . . . :  EMIG
Permissions  . . . . . :  *RW
Authorization list . . . :  *NONE
Require encryption . . . :  *NO
Maximum users  . . . . . :  *NOMAX
Current users  . . . . . :  1
Text 'description' . . . :  Chuck Emig user share
Path . . . . . :  /emig



Creation date/time . . . :  05/01/25 2:09:42 PM
Last change date/time  . :  05/01/25 2:09:42 PM
Last access date/time  . :  05/01/25 2:19:10 PM
Text converting CCSID  . :  *NONE
Text converting  . . . . :  *NONE
Number of extensions . . :  0
Extension  . . . . . :
```

NetServer Audit Records

IBM i

You can track security events related to IBM i NetServer using VP (Network) audit records.

The following VP audit record types can be used to track security events related to IBM i NetServer:

- **P –** Password error for a user profile that exists on the system
- **D –** IBM i NetServer user disabled

New in 7.5

- **A –** Authorization list (AUTL) permission failure for a user accessing the server or a share that is access–restricted by an authorization list

New in 7.6

- **C –** Server or share connection established
- **E –** Server or share connection ended
- **S –** Share added, modified, or removed
- **U –** Unknown user attempt to connect or guest connection

The IBM i NetServer VP audit records are controlled by different auditing level values. The various record types are listed below with the auditing level required to record them.

- *NETFAIL – A, D, P, and U
- *NETBAS – S
- *NETSMBSVR – C and E

VP-A Audit Records

VP-A audit records are generated when a user with below minimum authorization list authority attempts to connect to the server or a share restricted by an authorization list.

An audit record is not generated when share access is limited to read-only by the user only having *USE authority to the AUTL.


```
--
-- Find NetServer access blocked by AUTL restrictions in the last 7 days
--
select ENTRY_TIMESTAMP, AUDIT_USER_NAME, COMPUTER_NAME, SHARE_NAME, SHARE_AUTHORIZATION_LIST
  from table (
      SYSTOOLS.AUDIT_JOURNAL_VP(STARTING_TIMESTAMP => current timestamp - 7 days)
    )
    where ENTRY_TYPE like 'A'
    order by entry_timestamp desc;
```

ENTRY_TIMESTAMP	AUDIT_USER_NAME	COMPUTER_NAME	SHARE_NAME	SHARE_AUTHORIZATION_LIST
2025-05-01 16:38:46.519072	EMIGTEST	::ffff:10.234.200.123	*SERVER	NETSVRAUTL
2025-05-01 16:25:01.710496	EMIGTEST	::ffff:10.234.200.123	EMIG	NETSHRAUTL

VP-U Audit Records

IBM i

VP-U audit records are generated when a user attempts a connection with a user profile that doesn't exist on the system. If guest support is enabled, the record represents a guest connection to the server that was accepted. If not, the record represents an invalid user connection that was rejected.

VP-U audit records may be a symptom of a network attack on the server.

```
--
-- Find NetServer access attempts from unknown / guest users in the last day
--
select ENTRY_TIMESTAMP, AUDIT_USER_NAME, COMPUTER_NAME
  from table (
      SYSTOOLS.AUDIT_JOURNAL_VP(STARTING_TIMESTAMP => current timestamp - 24 hours)
    )
    where ENTRY_TYPE like 'U'
    order by entry_timestamp desc;
```

ENTRY_TIMESTAMP	AUDIT_USER_NAME	COMPUTER_NAME
2025-05-01 16:56:33.036224	HACKER	::ffff:10.234.200.123
2025-05-01 15:03:50.934944	BADGUY	::ffff:10.234.200.123

VP-S Audit Records

VP-S audit records are generated when a NetServer share is added, changed, or removed. The audit record includes the properties of the updated share.

```
--
-- Find information about shares of the IFS root ('/')
--
select ENTRY_TIMESTAMP, AUDIT_USER_NAME, SHARE_NAME, SHARE_ACTION, QUALIFIED_JOB_NAME, PATH_NAME
 from table (
    SYSTOOLS.AUDIT_JOURNAL_VP()
  )
  where PATH_NAME like '/'
  order by entry_timestamp desc;
```

ENTRY_TIMESTAMP	AUDIT_USER_NAME	SHARE_NAME	SHARE_ACTION	QUALIFIED_JOB_NAME	PATH_NAME
2025-05-01 14:57:38.526176	EMIG	BADROOT	REMOVE	798138/EMIG/QPADEV0008	/
2025-05-01 14:47:26.362224	EMIG	BADROOT	ADD	798138/EMIG/QPADEV0008	/

```
--
-- Find file shares that were added to the system in the last month
--
select ENTRY_TIMESTAMP, AUDIT_USER_NAME, SHARE_NAME, QUALIFIED_JOB_NAME, PATH_NAME
 from table (
    SYSTOOLS.AUDIT_JOURNAL_VP(STARTING_TIMESTAMP => current timestamp - 30 days)
  )
  where ENTRY_TYPE like 'S' and SHARE_TYPE like 'FILE' and SHARE_ACTION like 'ADD'
  order by entry_timestamp desc;
```

ENTRY_TIMESTAMP	AUDIT_USER_NAME	SHARE_NAME	QUALIFIED_JOB_NAME	PATH_NAME
2025-05-01 14:57:38.526176	EMIG	BADROOT	798138/EMIG/QPADEV0008	/

VP-C and VP-E Audit Records

IBM i

VP-C audit entries record the start of NetServer session and share connections.
VP-E audit entries record the end of server and share connections.

SMB tends to have a lot of short-lived connections that can cause a lot of connect and disconnect records to be generated. These entries have their own audit setting (*NETSMBSVR) to allow administrators to choose if this level of detail is required.

```
--
-- Find NetServer client activity in the last hour
--
select  ENTRY_TIMESTAMP, AUDIT_USER_NAME, COMPUTER_NAME, ENTRY_TYPE_DETAIL, SHARE_NAME,
     SHARE_TYPE, CORRELATION_ID, ENCRYPTION_REQUIRED, PERMISSIONS
  from table (
    SYSTOOLS.AUDIT_JOURNAL_VP(STARTING_TIMESTAMP => current timestamp - 1 hour)
   )
   where ENTRY_TYPE like 'C' OR ENTRY_TYPE like 'E'
   order by entry_timestamp asc;
```

ENTRY_TIMESTAMP	AUDIT_USER_NAME	COMPUTER_NAME	ENTRY_TYPE_DETAIL	SHARE_NAME	SHARE_TYPE	CORRELATION_ID	ENCRYPTION_REQUIRED	PERMISSIONS
2025-05-02 10:55:44.909808	EMIG	::ffff:10.234.200.123	Server or share connection established	*SERVER	SERVER	00000000000000011	NO	*RW
2025-05-02 10:55:44.990736	EMIG	::ffff:10.234.200.123	Server or share connection established	EMIG	FILE	00000000000000011	YES	*RW
2025-05-02 10:56:07.313088	EMIG	::ffff:10.234.200.123	Server or share connection ended	EMIG	FILE	00000000000000011	-	-
2025-05-02 10:56:07.404976	EMIG	::ffff:10.234.200.123	Server or share connection ended	*SERVER	SERVER	00000000000000011	-	-
2025-05-02 11:04:38.803328	EMIGTEST	::ffff:10.234.200.123	Server or share connection established	*SERVER	SERVER	00000000000000015	NO	*RW
2025-05-02 11:04:38.890496	EMIGTEST	::ffff:10.234.200.123	Server or share connection established	EMIG	FILE	00000000000000015	YES	*R
2025-05-02 11:05:55.488592	EMIGTEST	::ffff:10.234.200.123	Server or share connection ended	EMIG	FILE	00000000000000015	-	-
2025-05-02 11:05:55.572784	EMIGTEST	::ffff:10.234.200.123	Server or share connection ended	*SERVER	SERVER	00000000000000015	-	-
2025-05-02 11:11:56.619360	EMIG	::ffff:10.234.200.123	Server or share connection established	*SERVER	SERVER	00000000000000019	NO	*RW
2025-05-02 11:11:56.698400	EMIG	::ffff:10.234.200.123	Server or share connection established	EMIG	FILE	00000000000000019	YES	*RW
2025-05-02 11:12:56.122032	EMIG	::ffff:10.234.200.123	Server or share connection established	EMIGHOME	FILE	00000000000000019	NO	*RW
2025-05-02 11:13:10.341968	EMIG	::ffff:10.234.200.123	Server or share connection ended	EMIGHOME	FILE	00000000000000019	-	-
2025-05-02 11:13:21.150352	EMIG	::ffff:10.234.200.123	Server or share connection ended	EMIG	FILE	00000000000000019	-	-
2025-05-02 11:13:21.150432	EMIG	::ffff:10.234.200.123	Server or share connection ended	*SERVER	SERVER	00000000000000019	-	-

Open Conversation

Questions

Demo

For more information

IBM Sites:

IBM i Home Page	https://www.ibm.com/it-infrastructure/power/os/ibm-i
IBM Strategy Whitepaper	https://www.ibm.com/it-infrastructure/us-en/resources/power/i-strategy-roadmap/
IBM Client Success	https://www.ibm.com/it-infrastructure/us-en/resources/power/ibm-i-customer-stories/
Support Life Cycle	https://www.ibm.com/support/lifecycle/
License Topics	https://www-01.ibm.com/support/docview.wss?uid=nas8N1022087
IBM i Release Life Cycle	https://www.ibm.com/support/pages/release-life-cycle
IBM i TR Wikis	IBM i Technology Updates

For more information:

Blogs to follow

- TechChannel You and i (Steve Will)
- TechChannel: i Can (Dawn May)
- TechChannel: iTalk with Tuohy
- TechChannel: OpenYour i with Jesse Gorzinski
- IBM Db2 for i (Kent Milligan)
- IBM i Analytics Blog (Jon Westcott Jr)
- iSee with Scott and Tim

More to follow

@IBMservers
@COMMONug
@IBMChampions
@IBMSystemsISVs
@LinuxIBMMag
@OpenPOWERorg
@ITJungleNews
@SAPonIBMi
@SiDforIBMi
@IBMAIXeSupp
@IBMAIXdoc

Hashtags to Use

#IBMPower
#IBMi
#IBMAIX
#Power10
#LinuxonPower
#HANAonPower
#ITinfrastructure
#OpenSource
#HybridCloud

Special notices

IBM i

This document was developed for IBM offerings in the United States as of the date of publication. IBM may not make these offerings available in other countries, and the information is subject to change without notice. Consult your local IBM business contact for information on the IBM offerings available in your area.

Information in this document concerning non-IBM products was obtained from the suppliers of these products or other public sources. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. Send license inquires, in writing, to IBM Director of Licensing, IBM Corporation, New Castle Drive, Armonk, NY 10504-1785 USA.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

The information contained in this document has not been submitted to any formal IBM test and is provided "AS IS" with no warranties or guarantees either expressed or implied.

All examples cited or described in this document are presented as illustrations of the manner in which some IBM products can be used and the results that may be achieved. Actual environmental costs and performance characteristics will vary depending on individual client configurations and conditions.

IBM Global Financing offerings are provided through IBM Credit Corporation in the United States and other IBM subsidiaries and divisions worldwide to qualified commercial and government clients. Rates are based on a client's credit rating, financing terms, offering type, equipment type and options, and may vary by country. Other restrictions may apply. Rates and offerings are subject to change, extension or withdrawal without notice.

IBM is not responsible for printing errors in this document that result in pricing or information inaccuracies.

All prices shown are IBM's United States suggested list prices and are subject to change without notice; reseller prices may vary.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

Any performance data contained in this document was determined in a controlled environment. Actual results may vary significantly and are dependent on many factors including system hardware configuration and software design and configuration. Some measurements quoted in this document may have been made on development-level systems. There is no guarantee these measurements will be the same on generally-available systems. Some measurements quoted in this document may have been estimated through extrapolation. Users of this document should verify the applicable data for their specific environment.

Special notices (cont.)

Revised December 2, 2010