IBM

Tivoli Security Compliance Manager

Version 5.1.1 – April, 2007

Collector and Message Reference Windows Open SSH Addendum

IBM

Table of Contents

Preface

The *IBM Tivoli Security Compliance Manager Collector and Message Reference Addendum* describes the following:

- The Open SSH policy checks whether the configuration of the SSH server is compliant with the security requirements

Documentation for previously developed collectors that are used in File Integrity policy can be found in the *IBM Tivoli Security Compliance Manager Collector and Message Reference* publication.

The information in this book will be added to the *IBM Tivoli Security Compliance Manager Collector and Message Reference* publication the next time that publication is updated. This book is being used to provide documentation of new policies and new collectors until that time.

What this book contains

This document contains the following chapters:

- Chapter 1, Policies

    Provides information on the Open SSH policy.

Chapter 1.Policies

This chapter documents the following policy:

- Open SSH policy

Open SSH policy

The Open SSH policy checks the compliance of the Open SSH server configuration.

Deployment information for Open SSH policy template

The IBM Tivoli Security Compliance Manager Open SSH policy template consists of collectors and compliance queries that can be used to determine if a Open SSH configuration complies with specific security requirements.

See the *IBM Tivoli Security Compliance Manager Administration Guide* for details regarding installing and deploying policies.

Policy overview

The queries included in this policy check the following items:

- List of Clients Scanned
- List of Clients with Incorrect Platform
- Required Collector Data for any.any.OpenSSHV2
- Required Collector Data for win.any.FilePermsV2
- SSH AcceptEnv Restriction
- SSH Host-Based Authentication
- SSH KeepAlive Restriction
- SSH KeyRegenerationInterval Restriction
- SSH LogLevel Restriction
- SSH LoginGraceTime Restriction
- SSH MaxStartups Restriction
- SSH OSR ACL Restrictions
- SSH PasswordAuthentication Restriction
- SSH PermitEmptyPasswords Restriction
- SSH PermitRootLogin Restriction
- SSH PermitUserEnvironment Restriction

- SSH PrintMotd Restriction

- SSH Protocol Restriction

- SSH PubkeyAuthentication Restriction

- SSH RSAAuthentication Restriction

- SSH ServerKeyBits Restriction

- SSH StrictModes Restriction

Parameters used in the policy:

Parameter Name	Description	Type	Default
Max Collector Data Age	The maximum acceptable age of collector data in days.	Integer	8 [days]
Allowed Users	Users who are allowed to change the sshd config files	List of strings	SYSTEM

Configuring this policy for your deployment

To configure the Open SSH policy for your environment, do the following:

- update the FILE parameter of the win.any.FilePermsV2 collector so it meets your requirements (you have to specify where ssh files are located – there is a sample configuration applied)

- update the CONFIG_FILE parameter of the any.any.OpenSSHV2 collector so it meets your requirements (the collector will look for the sshd_config file in many different location – see any.any.OpenSSHV2 documentation)

- be aware that three compliance queries base on OpenSSH default setting (SSH ServerKeyBits Restriction, SSH AcceptEnv Restriction, SSH Protocol Restriction) which may differ in various versions of OpenSSH:

  - ServerKeyBits   768

  - AcceptEnv   no user environment variables are allowed

  - Protocol   2,1

Compliance queries

The following sections contain additional information on all of the compliance queries contained within the File Integrity policy.

List of Clients Scanned

List of Clients Snapshot was run against.

Table 1.List of Clients Scanned

Priority	Informational
Collector instance name	N/A

Violation message:

Client Snapshot Completed successfully: {1}

Note: The {1} in the message is replaced with the value of HOSTNAME as selected in the SQL.

SQL query:

```
SELECT
     a.cli_id, a.alias as "Hostname"
FROM
     jac_sys.clients a
```

List of Clients with Incorrect Platform

List of Clients Snapshot was run against that were the incorrect platform for this WINDOWS SSH policy.

Table 2.List of Clients with Incorrect Platform

Priority	Low
Collector instance name	N/A

Violation message:

Incorrect Client (hostname: {1}) Platform: {2}, should be WINDOWS SSH

Note: The {1} in the message is replaced with the value of HOSTNAME, {2} is replaced with the value of OS_NAME.

SQL query:

```
SELECT
     a.cli_id, a.alias as "Hostname", a.os_name
FROM
     jac_sys.clients a
Where
      a.os_name NOT LIKE 'Windows%'
```

Required Collector Data for any.any.OpenSSHV2

Verifies the required collector data for Policy checks has run successfully and Within X Days - any.any.OpenSSHV2.

Table 3.Required Collector Data for any.any.OpenSSHV2

Priority	Normal
Collector instance name	OpenSSHV2.

Violation message:

Required Collector Data missing or older than X days: any.any.OpenSSHV2.

where X is a value of 'Max Collector Data Age' policy parameter.

SQL query:

```
SELECT DISTINCT
      SCANED_CLI.cli_id,
      SCANED_CLI.alias AS "Hostname",
      'Required Collector Data missing or older than $(Max Collector Data Age) days:
            any.any.OpenSSHV2' AS "Message"
FROM
(
SELECT
      a.cli_id, a.alias
FROM
      jac_sys.clients a
) AS SCANED_CLI
WHERE
SCANED_CLI.cli_id IN
(
SELECT DISTINCT cli_id
FROM jac_data.openssh_main_v2
WHERE logdate &lt; timestamp(CHAR(CURRENT DATE - $(Max Collector Data Age) DAYS) ||
      '-00.00.00') OR logdate IS NULL
)
OR
cli_id NOT IN (SELECT DISTINCT cli_id FROM jac_data.openssh_main_v2 )
```

Required Collector Data for win.any.FilePermsv2

Verifies the required collector data for Policy checks has run successfully and Within X Days - win.any.FilePermsV2.

Table 4.Required Collector Data for win.any.FilePermsv2

Priority	Normal
Collector instance name	FilePermsV2

Violation message:

Collector Data missing or older than X days: win.any.FilepermsV2.

where X is a value of 'Max Collector Data Age' policy parameter.

SQL query:

```
SELECT DISTINCT
      SCANED_CLI.cli_id,
      SCANED_CLI.alias AS "Hostname",
      'Required Collector Data missing or older than $(Max Collector Data Age) days:
            any.any.OpenSSHV2' AS "Message"
FROM
(
SELECT
      a.cli_id, a.alias
FROM
      jac_sys.clients a
) AS SCANED_CLI
WHERE
SCANED_CLI.cli_id IN
(
SELECT DISTINCT cli_id
FROM jac_data.win_file_perms_v2
WHERE logdate < timestamp(CHAR(CURRENT DATE - $(Max Collector Data Age) DAYS) || '-00.00.00')
      OR logdate IS NULL
)
OR
cli_id NOT IN
(
SELECT DISTINCT cli_id FROM jac_data.win_file_perms_v2
)
```

SSH AcceptEnv Restriction

The AcceptEnv parameter in sshd_config must not exist.

Table 5.SSH AcceptEnv Restriction

Priority	Normal
Collector instance name	OpenSSHV2

Violation message:

Invalid setting (value: {2}) for sshd (processPID: {1}) parameter 'AcceptEnv': must not exist.

Note: The {1} in the message is replaced with the value of PROCESS_PID, {2} is replaced with the value of VARIABLE_PATTERN.

SQL query:

```
SELECT DISTINCT
      a.cli_id, a.process_pid as "PID", a.env_variable as "VARIABLE_PATTERN"
FROM
      jac_data.openssh_env_variable_v2 a
WHERE
      a.env_variable != '!default!'
```

SSH Host-Based Authentication

Host-Based Authentication - The /etc/hosts.equiv file must not be used to enable host-based authentication.

Table 6.SSH Host-Based Authentication

Priority	Normal
Collector instance name	OpenSSHV2

Violation message:

Invalid setting for sshd (processPID: {1}) parameter 'HostBasedAuthentication': {2}

Note: The {1} in the message is replaced with the value of PROCESS_PID, {2} is replaced with the text '/ETC/HOSTS.EQUIV must not be used as an access control mechanism'.

SQL query:

```
SELECT DISTINCT
       a.cli_id, a.process_pid as "PID", '/ETC/HOSTS.EQUIV must not be used as an access
control mechanism' AS Message
FROM
      jac_data.openssh_main_v2 a
WHERE
      a.Hostbased_Authentication=1
```

SSH KeepAlive Restriction

SSH KeepAlive - Configures the server to send TCP keepalive messages to the client and cleanup crashed sessions to prevent indefinitely hanging sessions. Value must be set to YES.

Table 7.SSH KeepAlive Restriction

Priority	Normal
Collector instance name	OpenSSHV2

Violation message:

Invalid setting (value: {2}) for sshd (processPID: {1}) in parameter 'TCPKeepAlive': must be set to YES

Note: The {1} in the message is replaced with the value of PROCESS_PID, {2} is replaced with the TCP_KEEP_ALIVE value.

SQL query:

```
SELECT DISTINCT
     a.cli_id, a.process_pid as "PID", a.tcp_keep_alive
FROM
     jac_data.openssh_main_v2 a
WHERE
     a.tcp_keep_alive = 0
```

SSH KeyRegenerationInterval Restriction

KeyRegenerationInterval (OpenSSH Only) The number of seconds that elapse between regenerations of the server's ephemeral key. KeyRegenerationInterval value must be 3600 or less and not zero.

Table 8.SSH KeyRegenerationInterval Restriction

Priority	Normal
Collector instance name	OpenSSHV2

Violation message:

Invalid setting (value: {2}) for sshd (processPID: {1}) in parameter 'TCPKeepAlive': must not be longer than 3600s

Note: The {1} in the message is replaced with the value of PROCESS_PID, {2} is replaced with the KEY_REGENERATION_INTERVAL value.

SQL query:

```
SELECT DISTINCT
     a.cli_id, a.process_pid as "PID", a.key_regeneration_interval
FROM  jac_data.openssh_main_v2 a
WHERE
     a.key_regeneration_interval > 3600 OR a.key_regeneration_interval = 0
```

SSH LogLevel Restriction

LogLevel (OpenSSH Only) Must be not null and it should be set to INFO, VERBOSE, DEBUG, DEBUG1, DEBUG2 or DEBUG3.

Table 9.SSH LogLevel Restriction

Priority	Normal
Collector instance name	OpenSSHV2

Violation message:

Invalid setting (value: {2}) for sshd (processPID: {1}) in parameter 'LogLevel': must be set to INFO or higher.

Note: The {1} in the message is replaced with the value of PROCESS_PID, {2} is replaced with the LOG_LEVEL value.

SQL query:

```
SELECT DISTINCT
      a.cli_id, a.process_pid as "PID", a.log_level
FROM
      jac_data.openssh_main_v2 a
WHERE
      UPPER(a.log_level) IN ('QUIET', 'FATAL', 'ERROR')
```

SSH LoginGraceTime Restriction

LoginGraceTime - The number of seconds before the server disconnect a session that has not been successfully authenticated. Value must be 120 or less.

Table 10.SSH LoginGraceTime Restriction

Priority	Normal
Collector instance name	OpenSSHV2

Violation message:

Invalid setting (value: {2}) for sshd (processPID: {1}) in parameter 'LoginGraceTime': must be set to 120 or less and must not be zero.

Note: The {1} in the message is replaced with the value of PROCESS_PID, {2} is replaced with the LOGIN_GRACE_TIME value.

SQL query:

```
SELECT DISTINCT
      a.cli_id, a.process_pid as "PID", a.login_grace_time
FROM
      jac_data.openssh_main_v2 a
WHERE
      a.login_grace_time > 120 OR a.login_grace_time = 0
```

SSH MaxStartups Restriction

MaxStartups (OpenSSH Only) The maximum number of simultaneous, unauthenticated sessions that can be open to the server. Value must be 100 or less.

Table 11.SSH MaxStartups Restriction

Priority	Normal
Collector instance name	OpenSSHV2

Violation message:

Invalid setting (value: {2}) for sshd (processPID: {1}) in parameter 'MaxStartups': must be set to 100 or less.

Note: The {1} in the message is replaced with the value of PROCESS_PID, {2} is replaced with the MAX_STARTUPS value.

SQL query:

```
SELECT DISTINCT
     cli_id, process_pid, max_startups
FROM
     (
     SELECT
          cli_id, process_pid, max_startups,
          case when max_startup like '%:%'
          then substr( max_startup, locate( ':', max_startup ) + 1 )
          else max_startups end as max_startup
     FROM (
          SELECT
               cli_id, process_pid, max_startups,
                    case when max_startups like '%:%'
               then substr( max_startups, locate( ':', max_startups ) + 1 )
               else max_startups end as max_startup
          FROM
               jac_data.openssh_main_v2
          ) a
     ) b
WHERE
     lower( max_startup ) != upper( max_startup )
     or int( max_startup ) > 100
```

SSH OSR ACL Restrictions

SSH Libraries Files and Configuration Files Permissions must not be world-writable if exists.

Table 12.SSH OSR ACL Restrictions

Priority	Normal
Collector instance name	FilePermsV2

Violation message:

Invalid SSH OSR ACL for {1}, must not be world-writable.

SQL query:

```
SELECT DISTINCT
      a.cli_id, a.file as "File"
FROM
      jac_data.win_file_perms_v2 a
WHERE (a.perms_type=-1 OR a.perms_type=1)
AND   (a.user_name NOT IN ($(Allowed Users)))
AND   (a.file_read_data=1
      OR    a.file_write_data=1
      OR    a.file_append_data=1
      OR    a.file_read_ea=1
      OR    a.file_write_ea=1
      OR    a.file_execute=1
      OR    a.file_delete_child=1
      OR    a.file_read_attribute=1
      OR    a.file_write_attribute=1
      OR    a.delete=1
      OR    a.read_control=1
      OR    a.write_dac=1
      OR    a.write_owner=1))
AND
      (a.file LIKE '%sshd_config'
      OR a.file LIKE '%ssh_host_key'
      OR a.file LIKE '%ssh_host_dsa_key'
      OR a.file LIKE '%ssh_host_rsa_key')
```

SSH PasswordAuthentication Restriction

Password Authentication permits to authenticate using a unique username and password.

Table 13.SSH PasswordAuthentication Restriction

Priority	Normal
Collector instance name	OpenSSHV2

Violation message:

Invalid setting (value: {2}) for sshd (processPID: {1}) in parameter 'PasswordAuthentication': must be set to 'yes'.

Note: The {1} in the message is replaced with the value of PROCESS_PID, {2} is replaced with the PASSWORD_AUTHENTICATION value.

SQL query:

```
SELECT DISTINCT
     a.cli_id, a.process_pid as "PID", a.password_authentication
FROM
     jac_data.openssh_main_v2 a
WHERE
     a.password_authentication = 0
```

SSH PermitEmptyPasswords Restriction

PermitEmptyPasswords - Allows login to accounts with empty password strings. Value must be set to NO.

Table 14.SSH PermitEmptyPasswords Restriction

Priority	Normal
Collector instance name	OpenSSHV2

Violation message:

Invalid setting (value: {2}) for sshd (processPID: {1}) in parameter 'PermitEmptyPasswords': must be set to 'no'.

Note: The {1} in the message is replaced with the value of PROCESS_PID, {2} is replaced with the PERMIT_EMPTY_PASSWORD value.

SQL query:

```
SELECT DISTINCT
     a.cli_id, a.process_pid as "PID", a.permit_empty_passwords
FROM
     jac_data.openssh_main_v2 a
WHERE
     a.permit_empty_passwords = 1
```

SSH PermitRootLogin Restriction

PermitRootLogin - Permits the root user to login remotely. Value must be set to NO or without-password. Unless mechanisms are in place to determine the identity of the individual accessing the system.

Table 15.SSH PermitRootLogin Restriction

Priority	Normal
Collector instance name	OpenSSHV2

Violation message:

Invalid setting (value: {2}) for sshd (processPID: {1}) in parameter 'PermitRootLogin': must be set to 'no' or 'without-password'.

Note: The {1} in the message is replaced with the value of PROCESS_PID, {2} is replaced with the PERMIT_ROOT_LOGIN value.

SQL query:

```
SELECT DISTINCT
      a.cli_id, a.process_pid as "PID", a.permit_root_login
FROM
      jac_data.openssh_main_v2 a
WHERE
      UPPER(a.permit_root_login) NOT IN ('NO', 'WITHOUT-PASSWORD' )
```

SSH PermitUserEnvironment Restriction

PermitUserEnvironment (OpenSSH 3.5 and greater) Permits processing of user environment files, which may allow users to bypass access restrictions. Value must be set to NO.

Table 16.SSH PermitUserEnvironment Restriction

Priority	Normal
Collector instance name	OpenSSHV2

Violation message:

Invalid setting (value: {2}) for sshd (processPID: {1}) in parameter 'PermitUserEnvironment': must be set to 'no'.

Note: The {1} in the message is replaced with the value of PROCESS_PID, {2} is replaced with the PERMIT_USER_ENVIRONMENT value.

SQL query:

```
SELECT DISTINCT
      a.cli_id, a.process_pid as "PID", a.permit_user_environment
FROM
      jac_data.openssh_main_v2 a
WHERE
      a.permit_user_environment = 0
```

SSH PrintMotd Restriction

Business Use Notice Required. PrintMotd value must be set to YES or default.

Table 17.SSH PrintMotd Restriction

Priority	Normal
Collector instance name	OpenSSHV2

Violation message:

Invalid setting (value: {2}) for sshd (processPID: {1}) in parameter 'PrintMotd': must be set to 'yes'.

Note: The {1} in the message is replaced with the value of PROCESS_PID, {2} is replaced with the PERMIT_MOTD value.

SQL query:

```
SELECT DISTINCT
      a.cli_id, a.process_pid as "PID", a.print_motd
FROM
      jac_data.openssh_main_v2 a
WHERE
      a.print_motd = 0
```

SSH Protocol Restriction

Protocol (OpenSSH Only) The SSH protocol(s) that are accepted by the server.. Value must be set to 2,1 or 2.

Table 18.SSH Protocol Restriction

Priority	Normal
Collector instance name	OpenSSHV2

Violation message:

Invalid setting for sshd (processPID: {1}) in parameter 'Protocol': must be set to '2,1' or 2.

Note: The {1} in the message is replaced with the value of PROCESS_PID, {2} is replaced with the PROTOCOL value.

SQL query:

```
SELECT DISTINCT a.cli_id, a.process_pid as "PID"
FROM
      jac_data.openssh_protocol_v2 a
EXCEPT
      SELECT DISTINCT
            b.cli_id, b.process_pid
      FROM
            jac_data.openssh_protocol_v2 b
      WHERE
            b.protocol='2' OR b.protocol='!default!'
```

SSH PubkeyAuthentication Restriction

PubkeyAuthentication (OpenSSH Only) Permits users to login using public/private key pairs. Value must be set to YES or default.

Table 19.SSH PubkeyAuthentication Restriction

Priority	Normal
Collector instance name	OpenSSHV2

Violation message:

Invalid setting (value: {2}) for sshd (processPID: {1}) in parameter 'PubkeyAuthentication': must be set to 'yes'.

Note: The {1} in the message is replaced with the value of PROCESS_PID, {2} is replaced with the PUBKEY_AUTHENTICATION value.

SQL query:

```
SELECT DISTINCT
      a.cli_id, a.process_pid as "PID", a.pubkey_authentication
FROM
      jac_data.openssh_main_v2 a
WHERE
      a.pubkey_authentication = 0
```

SSH RSAAuthentication Restriction

RSAAuthentication (OpenSSH Only) Permits users to login using public/private key pairs. Value must be set to YES or default.

Table 20.SSH RSAAuthentication Restriction

Priority	Normal
Collector instance name	OpenSSHV2

Violation message:

Invalid setting (value: {2}) for sshd (processPID: {1}) in parameter 'RSAAuthentication': must be set to 'yes'.

Note: The {1} in the message is replaced with the value of PROCESS_PID, {2} is replaced with the RSA_AUTHENTICATION value.

SQL query:

```
SELECT DISTINCT
      a.cli_id, a.process_pid as "PID", a.rsa_authentication
FROM
      jac_data.openssh_main_v2 a
WHERE
      a.rsa_authentication = 0
```

SSH ServerKeyBits Restriction

Transmission Encryption: ServerKeyBits value must be set to 128 or default.

Table 21.SSH ServerKeyBits Restriction

Priority	Normal
Collector instance name	OpenSSHV2

Violation message:

Invalid setting (value: {2}) for sshd (processPID: {1}) in parameter 'ServerKeyBits': must be set to at least 128.

Note: The {1} in the message is replaced with the value of PROCESS_PID, {2} is replaced with the SERVER_KEY_BITS value.

SQL query:

```
SELECT DISTINCT
      a.cli_id, a.process_pid as "PID", a.server_key_bits
FROM
      jac_data.openssh_main_v2 a
WHERE
      a.server_key_bits < 128 AND a.server_key_bits != -1
```

SSH StrictModes Restriction

StrictModes - Configures SSH to verify ownership and permissions of user files and home directories before allowing logins. Value must be set to YES.

Table 22.SSH StrictModes Restriction

Priority	Normal
Collector instance name	OpenSSHV2

Violation message:

StrictModes - Configures SSH to verify ownership and permissions of user files and home directories before allowing logins. Value must be set to YES.

Note: The {1} in the message is replaced with the value of PROCESS_PID, {2} is replaced with the STRICT_MODES value.

SQL query:

```
SELECT DISTINCT
      a.cli_id, a.process_pid as "PID", a.strict_modes
FROM
      jac_data.openssh_main_v2 a
WHERE
      a.strict_modes = 0
```

Collector Instances and Parameters

The table below associates each collector instance with a specific collector and lists any parameters it has and the values for those parameters. Each collector instance is scheduled to run once a day at a random time.

Table 23.Collector instances and parameters for OpenSSH policy

Instance name	Collector name	Parameter name	Parameter value
OpenSSHV2	any.any.OpenSSHV2	1. CONFIG_FILE	Parameters should be set accordingly to client's requirements, more information can be found in OpenSSHV2 documentation
FilePermsV2	win.any.FilePermsV2	1. FILENAME	

any.any.OpenSSHV2

1.0 Platforms

Any

2.0 Requirement this collector satisfies

The collector gathers information about configuration of every running OpenSSH server process.

3.0 Description

This collector gathers information from the configuration file (sshd_config) as well as from the initial options passed to the ssh server while starting up.

4.0 How data is collected

If the '-f' option is provided collector scans only specified configuration file. If the '-f' option is not set, the collector assumes that sshd_config is located in one of the default locations:

For Unix system

- /etc/ssh/sshd_config
- /etc/ssh/sshd2_config
- /etc/ssh2/sshd_config
- /etc/ssh2/sshd2_config
- /opt/etc/ssh/sshd_config
- /etc/sshd_config
- /etc/sshd2_config
- /etc/openssh/sshd_config
- /usr/local/etc/sshd_config
- /usr/local/etc/sshd2_config

For Windows system

- %OpenSSH_HomeDir%/etc/sshd_conf
- %OpenSSH_HomeDir%/etc/ssh/sshd2_config
- %OpenSSH_HomeDir%/etc/ssh2/sshd_config
- %OpenSSH_HomeDir%/etc/ssh2/sshd2_config
- %OpenSSH_HomeDir%/opt/etc/ssh/sshd_config
- %OpenSSH_HomeDir%/etc/sshd_config
- %OpenSSH_HomeDir%/etc/sshd2_config
- %OpenSSH_HomeDir%/etc/openssh/sshd_config
- %OpenSSH_HomeDir%/usr/local/etc/sshd_config
- %OpenSSH_HomeDir%/usr/local/etc/sshd2_config

If the file is not located in one of the above locations the collector would not be able to find it on it's own – in this case "CONFIG_FILE" parameter has to be provided. If the '-f' option is set and "CONFIG_FILE" parameter is set the collector will ignore the parameter, on the other way, if "CONFIG_FILE" is provided collector will look for sshd_config only in specified locations, will not scan default locations at all.

5.0 Specify any limitations.

If there is wrong value of the *Protocol* option (for example *Protocol* = "3, 2") specified either in the sshd_config or via command line the collector would return wrong value (in this case *Protocol* = "3, 2"), while the ssh server will ignore wrong protocol specification.

6.0 Parameters

Parameter	Description	Required	Default
CONFIG_FILE	If the location of the configuration file is different to the default one this parameters should be set.	No	/etc/ssh/sshd_config

7.0 Table Data

If some column contains "-*1*" or "*default*" it means that this option has not been specified and is set to default value.

OPENSSH_ALLOW_GROUPS_V2

Column	Description	Size	Type
PROCESS_PID	PID of a ssh server process		INT
PATTERN	groups name pattern that are allowed to use this ssh server	64	VARCHAR

OPENSSH_ALLOW_USERS_V2

Column	Description	Size	Type
PROCESS_PID	PID of a ssh server process		INT
PATTERN	user name patterns that are allowed to use this ssh server	64	VARCHAR

OPENSSH_DENY_GROUPS_V2

Column	Description	Size	Type
PROCESS_PID	PID of a ssh server process		INT
PATTERN	group name patterns that are disallowed to use this ssh server	64	VARCHAR

OPENSSH_DENY_USERS_V2

Column	Description	Size	Type
PROCESS_PID	PID of a ssh server process		INT
PATTERN	name patterns that are disallowed to use this ssh server	64	VARCHAR

OPENSSH_PORT_ADDRESS_V2

Column	Description	Size	Type
PROCESS_PID	PID of a ssh server process		INT
PORT	Specifies the port number that sshd listens on.		INT
LISTEN_ADDRESS	Specifies the local addresses sshd should listen on.	63	VARCHAR

OPENSSH_CIPHERS_V2

Column	Description	Size	Type
PROCESS_PID	PID of a ssh server process		INT
CIPHERS	Specifies the ciphers allowed for protocol version 2. Multiple ciphers must be comma-separated. The supported ciphers are 3des-cbc, aes128-cbc, aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr, aes256-ctr, arcfour, blowfish-cbc.	64	VARCHAR

OPENSSH_MAC_V2

Column	Description	Size	Type
PROCESS_PID	PID of a ssh server process		INT
MAC	Specifies the available MAC (message authentication code) algorithms.	64	VARCHAR

OPENSSH_PROTOCOL_V2

Column	Description	Size	Type
PROCESS_PID	PID of a ssh server process		INT
PROTOCOL	Specifies the protocol versions sshd supports.	64	VARCHAR

OPENSSH_SUBSYSTEM_V2

Column	Description	Size	Type
PROCESS_PID	PID of a ssh server process		INT

SUBSYSTEM	Configures an external subsystem SSH PROTOCOL VER 2 ONLY	64	VARCHAR
COMMAND_NAME	Specifies the command name of the subsystem	512	VARCHAR

OPENSSH_ENV_VARIABLE_V2

Column	Description	Size	Type
PROCESS_PID	PID of a ssh server process		INT
ENV_VARIABLE	Specifies the patterns of environment variables sent by the client will be copied into the session's environ. SSH PROTOCOL VER 2 ONLY	64	VARCHAR

OPENSSH_HOST_KEYS_V2

Column	Description	Size	Type
PROCESS_PID	PID of a ssh server process		INT
HOST_KEY	Specifies a file containing a private host key used by SSH. (/etc/ssh/ssh_host_rsa_key, /etc/ssh/ssh_host_dsa_key applicable to SSH PROTOCOL VER 2 ONLY)	512	VARCHAR

OPENSSH_MAIN_V2

Column	Description	Size	Type
PROCESS_PID	PID of a ssh server process		INT
PROCESS_COMMAND	Command ssh server has been run with	512	VARCHAR
ALLOW_TCP_FORWARDING	Specifies whether TCP forwarding is permitted. (1 – yes, 0 – no)		INT
AUTHORIZED_KEY_FILE	Specifies the file that contains the public keys that can be used for user authentication	512	VARCHAR
BANNER	The contents of the specified file are sent to the remote user before authentication is allowed. SSH PROTOCOL VER 2 ONLY	512	VARCHAR
CHALLENGE_RESPONSE_AUTH	Specifies whether challenge response authentication is allowed. (1 – yes, 0 – no)		INT

CLIENT_ALIVE_INTERVAL	Timeout interval in seconds after which if no data has been received from the client, sshd will send a client alive message, 0 means never. SSH PROTOCOL VER 2 ONLY (1 – yes, 0 – no)		INT
CLIENT_ALLOW_COUNT_MAX	Sets the number of client alive messages (see above) which may be sent without sshd receiving any messages back from the client.		INT
COMPRESSION	Specifies whether compression is allowed. (1 – yes, 0 – no)		INT
GATEWAY_PORTS	Whether remote hosts are allowed to connect to ports forwarded for the client. (1 – yes, 0 – no)		INT
GSS_API_AUTHENTICATION	Specifies whether user authentication based on GSSAPI is allowed. SSH PROTOCOL VER 2 ONLY (1 – yes, 0 – no)		INT
GSS_API_CLEANUP_CREDENTIALS	Specifies whether to automatically destroy the user's credentials cache on logout. SSH PROTOCOL VER 2 ONLY		INT
HOSTBASED_AUTHENTICATION	Specifies whether rhosts or /etc/hosts.equiv authentication together with successful public key client host authentication is allowed. SSH PROTOCOL VER 2 ONLY		INT
IGNORE_RHOST	Specifies that .rhosts and .shosts files will not be used in RhostsRSAAuthentication or HostbasedAuthentication. (1 – yes, 0 – no)		INT
IGNORE_USER_KNOWN_HOSTS	Specifies whether sshd should ignore the user's $HOME/.ssh/known_hosts during RhostsRSAAuthentication or HostbasedAuthentication. (1 – yes, 0 – no)		INT
KERBEROS_AUTHETICATION	Specifies whether the password provided by the user for PasswordAuthentication will be validated through the Kerberos KDC. (1 – yes, 0 – no)		INT

KERBEROS_GET_AFS_TOKEN	If AFS is active and the user has a Kerberos 5 TGT, attempt to acquire n AFS token before accessing the user's home directory. (1 – yes, 0 – no)		INT
KERBEROS_OR_LOCAL_PASSWD	if password authentication through Kerberos fails then the password will be validated via any additional local mechanism such as /etc/passwd. (1 – yes, 0 – no)		INT
KERBEROS_TICKET_CLEANUP	Specifies whether to automatically destroy the user's ticket cache file on logout. (1 – yes, 0 – no)		INT
KEY_REGENERATION_INTERVAL	After this many sec of connection the key will be automatically regenerated.		INT
LOGIN_GRACE_TIME	The server disconnects after this many seconds if the user has not successfully logged in.		INT
LOG_LEVEL	Gives the verbosity level that is used when logging messages from sshd. (QUIET, FATAL, ERROR, INFO, VERBOSE, DEBUG, DEBUG1, DEBUG2 and DEBUG3)	16	VARCHAR
MAX_AUTH_TRIES	Maximum number of authentication attempts permitted per connection.		INT
MAX_STARTUPS	Maximum number of concurrent unauthenticated connections	16	VARCHAR
PASSWORD_AUTHENTICATION	Specifies whether password authentication is allowed. (1 – yes, 0 – no)		INT
PERMIT_EMPTY_PASSWORDS	Specifies whether empty password allowed. (1 – yes, 0 – no)		INT
PERMIT_ROOT_LOGIN	Specifies whether root can login using ssh(1). The argument must be "yes", "without-password", "forced-commands-only" or "no".	64	VARCHAR
PREMIT_USER_ENVIRONMENT	Specifies whether ~/.ssh/environment and environment= options in ~/.ssh/authorized_keys are processed by sshd. (1 – yes, 0 – no)		INT

PID_FILE	Specifies the file that contains the process ID of the sshd daemon.	512	VARCHAR
PRINT_LAST_LOG	Specifies whether sshd should print the date and time when the user last logged in. (1 – yes, 0 – no)		INT
PRINT_MOTD	Specifies whether sshd should print /etc/motd when a user logs in interactively. (1 – yes, 0 – no)		INT
PUBLEY_AUTHENTICATION	Whether public key authentication is allowed. SSH PROTOCOL VER 2 ONLY (1 – yes, 0 – no)		INT
RHOSTS_RSA_AUTHENTICATION	Specifies whether rhosts or /etc/hosts.equiv authentication together with successful RSA host authentication is allowed. SSH PROTOCOL VER 1 (1 – yes, 0 – no)		INT
RSA_AUTHENTICATION	Specifies whether pure RSA authentication is allowed. SSH PROTOCOL VER 1. (1 – yes, 0 – no)		INT
SERVER_KEY_BITS	Defines the number of bits in the ephemeral protocol version 1 server key. SSH PROTOCOL VER 1 ONLY		INT
SHOW_PATCH_LEVEL	Specifies whether sshd will display the patch level of the binary in the identification string. \ SSH PROTOCOL VER 1 ONLY (1 – yes, 0 – no)		INT
STRICT_MODES	Specifies whether sshd should check file modes and ownership of the user's files and home directory before accepting login. (1 – yes, 0 – no)		INT
SYSLOG_FACILITY	Gives the facility code that is used when logging messages from sshd. (DAEMON, USER, AUTH, LOCAL0, LOCAL1, LOCAL2, LOCAL3, ..., LOCAL7).	16	VARCHAR
TCP_KEEP_ALIVE	Specifies whether the system should send TCP keepalive messages to the other side. (1 – yes, 0 – no)		INT
USE_DNS	Specifies whether sshd should lookup the remote host name. (1 – yes, 0 – no)		INT

USE_LOGIN	Specifies whether login is used for interactive login sessions. (1 – yes, 0 – no)		INT
USE_PAM	Enables the Pluggable Authentication Module interface. (1 – yes, 0 – no)		INT
USE_PRIVILEGE_SEPARATION	Specifies whether sshd separates privileges by creating an unprivileged child process to deal with incoming network traffic. (1 – yes, 0 – no)		INT
X11_DISPLAY_OFFSET	Specifies the first display number available for sshd's X11 forwarding		INT
X11_FORWARDING	Specifies whether X11 forwarding is permitted. (1 – yes, 0 – no)		INT
X11_USE_LOCALHOST	Specifies whether sshd should bind the X11 forwarding server to the loopback address or to the wildcard address. (1 – yes, 0 – no)		INT
X_AUTH_LOCATION	Specifies the full pathname of the xauth(1) program.	512	VARCHAR
IPV4_ONLY	IP version sshd uses (1 – yes, 0 – no)		INT
IPV6_ONLY	IP version sshd uses (1 – yes, 0 – no)		INT
IS_DEAMON	Specifies whether it is run as a deamon. (1 – yes, 0 – no)		INT
IS_LOGGING	Specifies whether logs to a log file. (1 – yes, 0 – no)		INT

8.0 Error Messages

Message ID	Message	Description
HCVHC0002E	An error occurred reading the file <file>	If there is not enough permissions to read the configuration file
HCVHC0003E	File <file name> does not exist.	If the configuration file doesn't exist
HCVHC0007E	An error occurred while reading the output from the {0} command.	Collector is not able to parse the output of the script correctly.
HCVHC0013E	An error occurred when attempting to read the output from the following executable file: <executable file>.	If the output of the script does not meet the specification required by the collector
HCVHC0014E	The <executable name> executable file returned the following error message: <error message>.	The script returns anything to its stderr stream

HCVHC0028W	An entry that is not valid was found in the file {0}. The unrecognized entry is: {1}	Check if the specified sshd parameter is set correctely

9.0 Additional comments

- If there is wrong value for parameter *Protocol* provided either in configuration file or in command line the collector will gather this value whilst the sshd server will ignore the wrong one and take only the correct one (the collector would return every value).

- The *MaxStartups* parameter is always read from configuration file if it's there specified in other way collector returns the value from command line if it's there specified.

- If the collector is being run on AIX OS please be informed that AIX allows deleting the parameters the process has been run with. This means that if there would be any parameters passed by command line, collector will miss it.

win.any.FilePermsV2

1.0 Platforms

Windows

2.0 Requirement this collector satisfies

This collector returns the file information including file size, version, date when it is last modified and access permissions for all the specified files.

3.0 Description

Returns all User permissions and version for the directories and files specified as parameter.

Commands: PartInfo.exe, VersionInfo.exe, FilePerms.exe

FILENAME parameter can take multiple values.

4.0 How data is collected

This collector uses executable 'VersionInfo.exe' to get the file version. The executable 'FilePerms.exe' is used to get effective file permissions for all users of the file. If collector is not able to get effective rights due to some error, explicit rights are gathered and error code is put in the ERROR_CODE column. The executable 'PartInfo.exe' is used to find which are the local and remote file systems.

If an error occurs while collecting data for a file, then a message is logged and processing continues for the other files. Both tables WIN_FILES_V2 and WIN_FILE_PERMS_V2 are populated with null values for columns other than FILE_NAME and ERROR_CODE.

If file name specified as parameter does not exist, then There is no entry for that file in both the tables WIN_FILES_V2 and WIN_FILE_PERMS_V2.

If a file has no permissions set for any user, then in the WIN_FILES_V2 TIMESTAMP and VERSION column will have null values and in the WIN_FILE_PERMS_V2 only FILE_NAME and ERROR_CODE will be set all other column will be filled with null value.

If SCAN_LOCAL (or SCAN_REMOTE) parameter is set to false and the FILENAME parameter has a corresponding entry for a file on that file system, then that file will not be processed and a warning message will be logged indicating this. If that FILENAME parameter entry has a wildcard then it will not be expanded since that entire drive need not be scanned. Both the tables WIN_FILES_V2 and WIN_FILE_PERMS_V2 will not have any values for this entry.

The parameter FILENAME can contain entries using system environment variables. In such cases, the windows set command will be used to determine the values of the system environment variables. If a corresponding value is not provided by the set command then a warning message is logged and that file is not processed. As a result no data is populated in the tables WIN_FILES_V2 and WIN_FILE_PERMS_V2 for this file.

While giving values to the FILENAME parameter care should be taken while giving a drive name as parameter. In such a case the drive letter should be followed by a colon (:) and a backslash (\). The reason is that if the backslash is omitted and the current directory happens to be on that drive, then the collector will take the FILENAME as the current directory.

5.0 Specify any limitations.

N/A

6.0 Parameters

Parameter	Description	Required	Default
FILENAME	File name for which permissions are to be returned. The file name can be any of the following: - Fully qualified path. - File/ directory name without the fully qualified path (this will be searched for in the current directory). - File names which use environment variables. Environment variables such as SystemRoot and SystemDrive can be given by using the '%' symbol before and after the variable - File names which contain wildcards.	Yes	None
SCAN_LOCAL	Value indicating if local filesystem is to be scanned to get file / directory information	No	1 (True)
SCAN_REMOTE	Value indicating if remote filesystem is to be scanned to get file / directory information	No	1 (True)

7.0 Table Data

WIN_FILES_V2

Column	Description	Size	Type
FILE_NAME	Name of the input file.	256	VARCHAR
TIMESTAMP	Timestamp of last modification in file	0	TIMESTAMP
VERSION	File version, or "-" if file version does not exist, or null if version cannot be obtained	32	VARCHAR
SIZE	File size in bytes	0	BIGINT
MS_API_ERROR_CODE	Value returned by the executables (more detail information can be found in winerr.h)	0	INTEGER

WIN_FILE_PERMS_V2

Column	Description	Size	Type
FILE_NAME	File's name	256	VARCHAR
USER_NAME	User name	1024	VARCHAR
PERMS_TYPE	Indicates the type of the permissions gathered by the collector (-1 effective; 0 deny; 1 allow)	0	SMALLINT
FILE_READ_DATA	Permission to read from a file, or list the contents of a directory.	0	SMALLINT
FILE_WRITE_DATA	Permission to write to a file, or create a new file inside a directory.	0	SMALLINT
FILE_APPEND_DATA	Permission to append data to a file, create a new subdirectory inside a directory, or create a pipe instance.	0	SMALLINT
FILE_READ_EA	Permission to read extended attributes	0	SMALLINT
FILE_WRITE_EA	Permission to write extended attributes	0	SMALLINT
FILE_EXECUTE	Permission to execute a file or access a directory	0	SMALLINT
FILE_DELETE_CHILD	Permission to delete a file from a directory	0	SMALLINT
FILE_READ_ATTRIBUTE	Permission to read attributes	0	SMALLINT
FILE_WRITE_ATTRIBUTE	Permission to write attributes	0	SMALLINT
DELETE	Permission to delete a file or directory.	0	SMALLINT
READ_CONTROL	Permission to read permissions.	0	SMALLINT
WRITE_DAC	Permission to write permissions	0	SMALLINT
WRITE_OWNER	Permission to take ownership	0	SMALLINT
SYNCHRONIZE	Permission to use object for synchronization	0	SMALLINT
MS_API_ERROR_CODE	Value returned by the executables (more detail information can be found in winerr.h)	0	INTEGER

8.0 Error Messages

Message ID	Message	Description
HCVHC0000E in com.ibm.jac.msg.CollectorMessages	The <collector name> collector encountered an exception in the <method name> method. The following exception was not handled: <exception name>	Some unexpected error occurred while executing the collector.
HCVHC0006E in com.ibm.jac.msg.CollectorMessages	An error occurred running the <command name> command	Error occurred while running the command.
HCVHC0007E in com.ibm.jac.msg.CollectorMessages	An error occurred while reading the output from the <command name> command	Error occurred while reading command output.
HCVHC0008E in com.ibm.jac.msg.CollectorMessages	Required parameter <parameter name> is missing.	A parameter that is required for the collector to run is missing or contains no value.
HCVHC0010E in com.ibm.jac.msg.CollectorMessages	Parameter <parameter name> cannot have more than one value.	A parameter has been specified with more than one value when only a single value is allowed.
HCVHC0011W in com.ibm.jac.msg.CollectorMessages	File <filename> does not exist.	The file whose properties are to be determined does not exist
HCVHC0012E in com.ibm.jac.msg.CollectorMessages	An error occurred attempting to run the following executable file: <executable name>.	An unexpected error occurred while running the specified custom executable.
HCVHC0013E in com.ibm.jac.msg.CollectorMessages	An error occurred when attempting to read the output from the following executable file: <executable name>.	An unexpected error occurred when attempting to read the output from a custom executable.
HCVHC0015E in com.ibm.jac.msg.CollectorMessages	Both the <parameter name> and <parameter name> parameters have been set to 0 (false). At least one must be set to 1 (true).	Both parameters, SCAN_LOCAL and SCAN_REMOTE, have been set to 0 (false). At least one of these parameters must be set to 1 (true).
HCVHC0016E in com.ibm.jac.msg.CollectorMessages	An error occurred while setting the <stdout/stderr> to binary mode in the following executable file: <executable name>.	The binary mode could not be set in the specified executable file.
HCVHC0017E in com.ibm.jac.msg.CollectorMessages	An error occurred while running the <api name> API in the <executable filename> executable file. The following system error code was returned: <error code>.	An error occurred running the specified API in the specified executable program.
HCVHC0018E in com.ibm.jac.msg.CollectorMessages	Unexpected output was returned by the <command name> command. The unexpected data was: <data>.	The command specified returned unexpected data.
HCVHC0025E in com.ibm.jac.msg.CollectorMessages	A memory allocation error occurred in the <executable name> executable file.	Memory could not be allocated by the specified executable file.

HCVHC0036W in com.ibm.jac.msg.CollectorMessages	An incorrect value <value> for parameter <parameter name> was specified.	A parameter specified contained an incorrect value.
HCVHC0038W in com.ibm.jac.msg.CollectorMessages	An unknown environment variable <environment variable> was found in the path of file <file name>.	The file path contained an unknown environment variable.
HCVHC0041W in com.ibm.jac.msg.CollectorMessages	An error occurred while running the <API name> API in the <executable name> executable file for the file <file name>. The error code returned was: <error code>.	An error occurred running the specified API for the given file in the specified executable program.
HCVHC0046W in com.ibm.jac.msg.CollectorMessages	A security descriptor without a DACL was found while getting the file permissions for file <file name>.	While obtaining file permissions for the specified file, a security descriptor was found without a discretionary access control list (DACL).
HCVHC0047W in com.ibm.jac.msg.CollectorMessages	Incorrect SID encountered while obtaining the file permissions for file <file name>.	A security identifier (SID) that is not valid was encountered while getting file permissions.
HCVHC0048W in com.ibm.jac.msg.CollectorMessages	Unknown ACE type encountered while obtaining the file permissions for file <file name>.	An unknown access control entry (ACE) type was encountered while getting the file permissions for the specified file.
HCVHC0049W in com.ibm.jac.msg.CollectorMessages	Unable to process the specified file: {0}. The file is located on a {1} file system and processing for that type of file system is not enabled.	Processing for either the local or remote file systems has been disabled by the user. However, the file specified as a parameter is located on that type of file system.
HCVHC0050W in com.ibm.jac.msg.CollectorMessages	An error occurred attempting to run the following executable file: <executable file name> for the following file: <file name>.	An unexpected error occurred while running the specified executable file.
HCVHC0051W in com.ibm.jac.msg.CollectorMessages	A memory allocation error occurred in the <executable name> executable file for the file <filename>.	Memory could not be allocated in the specified executable program which was run for the given file.
HCVWA0209E	Incorrect value for parameter <parameter name> specified. Valid values are 0 or 1.	Parameter can be 0 or 1 only.
HCVWA0212W	An exception occurred when obtaining the version of file: <filename>.	Exception occurred while getting the Version of file.

Appendix.Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594
U.S.A

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758
USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program describe in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Customers are responsible for ensuring their own compliance with various laws such as the Graham-Leach-Bliley Act, the Sarbanes-Oxley Act, and the Health Insurance Portability and Accountability Act. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal, accounting or auditing advice, or represent or warrant that its products or services will ensure that customer is in compliance with any law.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

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

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Additional notices

THIRD PARTY LICENSE TERMS AND CONDITIONS, NOTICES AND INFORMATION

The license agreement for this product refers you to this file for details concerning terms and conditions applicable to third party software code included in this product, and for certain notices and other information IBM must provide to you under its license to certain software code. The relevant terms and conditions, notices and other information are provided or referenced below. Please note that any non-English version of the licenses below is unofficial and is provided to you for your convenience only. The English version of the licenses below, provided as part of the English version of this file, is the official version.

Notwithstanding the terms and conditions of any other agreement you may have with IBM or any of its related or affiliated entities (collectively "IBM"), the third party software code identified below are "Excluded Components" and are subject to the following terms and conditions:

(a) the Excluded Components are provided on an "AS IS" basis;

(b) IBM DISCLAIMS ANY AND ALL EXPRESS AND IMPLIED WARRANTIES AND CONDITIONS WITH RESPECT TO THE EXCLUDED COMPONENTS, INCLUDING, BUT NOT LIMITED TO, THE WARRANTY OF NON-INFRINGEMENT OR INTERFERENCE AND THE IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE;

(c) IBM will not be liable to you or indemnify you for any claims related to the Excluded Components; and

(d) IBM will not be liable for any direct, indirect, incidental, special, exemplary, punitive or consequential damages with respect to the Excluded Components.

Notice for Apache Software Foundation

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

Notice for the MD5 Message-Digest Algorithm MD5 Message-Digest Algorithm.

The Program includes software developed by RSA Data Security, Inc. The portions of the Program which are based on software developed by RSA Data Security, Inc. are Copyright (c) 1991-2 RSA Data Security, Inc. All rights reserved. IBM obtained the MD5 Message-Digest Algorithm under the terms and conditions of the following license from RSA Data Security, Inc.:

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

Trademarks

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

AFS
AIX
DB2
DB2 Universal Database
Domino
IBM
IBM logo
iSeries
pSeries
Lotus
SmartSuite
Tivoli
Tivoli logo
WebSphere
xSeries
zSeries

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.