EPING March 2007

This is an archived edition of EPing, first published in March 2007. Although every effort has been made to preserve the original content, errors may have crept in and links may no longer be available.

PING!

The HP User Group Technical Journal

From The Chair -

Going Up!

You are in a lift with your boss. As the doors close she says "I have this order request to renew our membership of hpUG. What benefits do we get from this?" You have 60 seconds until the lift reaches the tenth floor to convince her. Go!

As you are reading this I'm assuming you are already a member, and that you do find hpUG membership useful. But how do you demonstrate that? Are you a member because of the events programme, or because you find E-PING useful? Do you take advantage of the discount on courses we offer with HP Education, or is meeting with your peers and sharing experiences and best practice where you realise the greatest value? Maybe hpUG helps you through the maze of information that is out there to find the answers you need, or maybe it is something else entirely that you find useful.

We all have to demonstrate value for money these days as costs are closely monitored. This includes hpUG. Anecdotally we know you appreciate the services we offer but it would help us in driving the organisation forward if we could collect together your testimonials and experiences of how the User Group has helped your business. It doesn't have to be long – a sentence or two would really help. With your permission we would then be in a position to share your experiences with potential members and others who are assessing the value for money of joining the hpUG community. We could also share your comments with existing members – and it just might give you a few bullet points for that critical minute in the lift!

Please mail all comments (good or bad) to admin@hpug.org.uk

I look forward to hearing from you.

John Owen
HPUG Chairman

The Bluffer's Guide to OpenVMS Backup

Or, everything you wanted to know but were too shy to ask!

Few operating systems come with a fully featured backup and restore facility, but OpenVMS is one of them. However it is also easy not to make the best of the facility, or even abuse it. This article will look at a number of aspects of the use of BACKUP by examining the implications of a number of the qualifiers, and the effects of using the default settings, and how tuning for backup performance can also saturate or even overload your system.

What will also be looked at are some common misconceptions, and why you **should** use /IMAGE on ORACLE (and other) databases!

The objective is to make sure you have a backup that is useful and you can rely on. It is very easy, too easy to spend long periods performing backups that if actually used cannot faithfully recreate the environment. It is always a good idea to test your backups from a "bare metal" restoration perspective.

First, a brief look at the different types of backup you can make.

What is an /IMAGE backup?

Sometimes also known as a full backup, but only the IMAGE qualifier makes it so. This type of backup not only stores all the data (files) on a disc, it also saves the volume structure and its security. Therefore this includes the original settings which first initialised the disc, and the security characteristics (ownership, ACLs, etc.) contained within the root directory [000000]. When a system disc is involved, it also correctly updates the boot block to point at the system initialization EXE. File aliases (VMS$COMMON vs. SYS$COMMON) are also handled but are a separate topic in this article.

If you make an image backup you are saving faithfully the disk and file structure along with its associated security. One of the most common mistakes made is restoring a disk which is not made from a /IMAGE backup saveset. The main problem is that root level security is not restored. The other issues are that the volume cluster size and other initialization settings are not restored. An additional issue is you can run out of disk space as on a system disc, the common file structure is restored multiple times. Fixing this fault involves doing selective restores from the backup save set, and entering a file alias for the common root into the system specific directory, and optionally rewriting the boot block. Image backups also faithfully cope with moving data between different sized disks.

What is an /INCREMENTAL backup?

To be fair this is a restore qualifier which directs BACKUP to take the information in the backup saveset and update a disk structure. For example, you restore a backup from the last image with the /RECORD qualifier, then apply the saveset(s) created with the /SINCE=BACKUP/RECORD qualifiers (differential backup). This will update and remove the files which were deleted since the image or full backup, and put the newly created files onto the disk. The maximum data you can lose is up to the last good full and incremental backup set. (Note there is a known potential data loss situation with incremental backups with unpatched version 6 and earlier versions).

What is a /FULL backup?

This does NOT affect the backup at all, it is an output qualifier for the /LIST. DO NOT use /FULL in the belief it is making an image copy of your disk!

What is a /PHYSICAL backup?

This is a non file structured, block for block copy of the contents of a disk device. Each of the blocks on a disk are numbered from 0 to the maximum size of the disk (also known as the LBN – Logical Block Number) and the backup formed or copied using this qualifier is merely the data in each block. It is NOT possible to select files, and when using this, there is an implied /IGNORE=INTERLOCK applied, so if data changes on the disk during the backup operation, there is a high chance that the data has lost its integrity (i.e. is corrupted). There are three cases where this sort of backup will help. Firstly, it is extremely fast, there is no head movement on the disk (no file level scanning) so speed is limited to that of the output device. Secondly, when copying from disk to like disk with exclusive access (a separated shadow set or privately mounted disk) likewise it is extremely fast, but there is no defragmentation that you would get from an IMAGE backup. However it allows you to make a copy of a disk before you apply some structure-changing commands, such as using ANALYSE to repair a disk structure, or even apply some rather more dangerous fixes to files, directories and disk structures. The implication of course is you may copy any disk, regardless if BACKUP is able to access the file structure. Thirdly, performing a BACKUP/PHYSICAL to a disk which will be added to a shadow set can considerably speed up the COPY operation (please see earlier PING article about Shadowing and mirroring for details).

What does /IGNORE=INTERLOCK do?

Quite simply it allows backup to save data in the file while it is being written to or updated by other processes on the system or cluster. This, similar to the physical backup above, does mean that data files are likely to be corrupted, especially relational databases where each file gets stored with data that does not correspond to data stored when other files went into the backup saveset.
However it has a purpose in that most database applications make their own (usually disk to disk) clean application levels backups, so the corrupted data from the saveset would be replaced with good clean data. However you will have (if making an IMAGE backup) taken all the file attributes and file protections which will be inherited by the restored database files.

As an example, take an ORACLE relational database split across 5 disks including a transaction log disk. If a disk fails, you can have the hardware replaced, restore the database files from the last good backup, and replay the transaction log file(s). The problem is if you do not start to restore the database disks from an IMAGE backup with data backed up regardless of open state (/IGNORE=INTERLOCK), you lose all the security and ownership information, and replicating this, or trying to recreate it becomes an obstacle to restoring the database service. In worst cases ORACLE fails to start properly (but often is given BYPASS privilege so some effects are artificially lessened) but worse effects are user level based operations that fail mysteriously and require some effort to trapping security messages and trial and error and discussion with applications staff (some with failing memories) as to how it was originally configured! I speak from experience.

It is common for database vendors to tell you “not to waste time” making image backups as in their eyes they are useless. However they are not seeing this from the system manager’s perspective, and I hope that anyone reading this will check their procedures to make sure they are not going to fall into the above trap.

Why doesn’t BACKUP device:[*…]*.*;* work?

The file specification is exclusive of the [000000] master file directory. UIC and in many cases ACL based protection rely on a parent style relationship to the top level directories help in the [000000] directory, as well as a relationship with the volume owner information. Without a /IMAGE qualifier, those top level directories and volume ownership default to the username restoring the backup.

/OWNERSHIP=ORIGINAL can help, but often gets confused because /OWNERSHIP=PARENT is mutually exclusive but file ownership and permissions are often mixed up but nonetheless functional, and different bits of the database or user access break accordingly. Pathworks or Advanced Server often relies on embedded ACLs that are not properly propagated unless an image restore of a disk is being used.

Hopefully I have now convinced you that you should ignore the wisdom of your database vendors, and make your image backups with /IGNORE=INTERLOCK. Remember, database developers live in a made up test world, and rarely, if ever, have to deal with a "MUST" get data back and working in the real world.

Using /RECORD and /SINCE=BACKUP

These qualifiers allow you to mark the BACKUP date on files on the disk in question, and allow BACKUP to select files based on "now" and the last time the file was backed up. For data restoration, restore the last image backup (/RECORD), then apply the backup savesets made using the /SINCE=BACKUP. They will populate the disk with the new and updated files. There is a caveat…

OpenVMS Backup 6.2 changes

/ALIAS and /SINCE=BACKUP discussion

The /SINCE=BACKUP behaviour has been altered in that if a directory was modified (e.g. renamed) then the files in it will also be backed up. This preserves the contents (files) in that directory that may not have otherwise been recorded as being present in the newly named directory. Another change was in the alias directory processing. Supported versions of BACKUP have been patched, but beware if you are running an older and unpatched version that you could lose files. Another issue, more seen on ODS2 system disks, for restoration of files on later VMS versions, using /NOALIAS in the backup line will ensure that the files which are in the "real" directory and not the alias directory are properly backed up. Some restoration issues are quite commonly seen, so the author's advice (contravening HP's documented advice!) is to use /NOALIAS to enable backup savesets to be easily transportable. This is seen when (for example) booting a V7 operating system disk to restore a V6 or earlier system disk, and recovery from this is 'involved'. Therefore be aware that on versions 6.1 and earlier and circa 7.0, you may experience some backup and restoration issues in certain circumstances. The support landing zone versions of all VAX and Alpha 6.2 patches and VAX and Alpha latest 7.3 patches have the changes incorporated.

Tape media compaction

One issue often seen is the failure of compressed tape devices to use compression, or compaction. This is a hardware based compression which is equated to an approximate 2 to 1 compression. Some files (e.g. text) compress very well, others (e.g. already compressed files such as ZIP files) actually increase very slightly in size. The issue is around device drivers and their updates, and hardware and host commands that are recognised to achieve this. Some certain rare combinations are not supported and host commands to compress will always be ignored. However the following can help get the device and tape so that compression is enabled.

INIT/MEDIA=COMPACTION

This will make sure that the tape header is written with compression.

MOUNT/MEDIA=COMPACTION

Similarly instructs the tape device to soft enable compression.

BACKUP… /MEDIA=COMPACTION

This MUST be used if using the /REWIND qualifier, but also directs BACKUP to instruct, not so much the first tape volume, but the second, third and so on volumes to also be compressed. Ideally INIT all the tapes first with compaction before use – and with the correct and expected labels!

To /IGNORE=LABEL or /LABEL=(TAPE1,TAPE2,TAPE3) ?

To be frank it is sheer laziness that means many command procedures use /IGNORE=LABEL. This can significantly aid your backup integrity procedures and prevent "little accidents". Many system managers do not use label processing out of habit. When it was introduced around version 5, changing the existing behaviour, it was seen as an annoyance to be worked around using the /IGNORE=LABEL

The very simple example given above of using a list of label names is one simple way of directing tape labels for subsequent volumes. You can use a command sequence in your backup script to generate MON, TUE, WED, or MLY307 which represents a monthly for March (third month) in 2007. You can use your own coding system, 6 characters are plenty. Remember that unless specified, the second volume label defaults to the first four characters of the first label (driven by the first saveset name) with 02, 03 etc. appended.

What in practice you are avoiding is "tape label does not match one requested" but this can prevent the overwriting of a previously made backup. If you sensibly use tape labels then you avoid overwriting backup tapes which are not correctly labelled for the backup cycle, and using the /REWIND with the /TAPE_EXPIRATION, you can protect tapes from being overwritten too soon in case they do have similar labels. For example you may have 4 or 5 sets of daily tapes with the labels MONDAY, TUEDAY, etc., (sic) with little coloured tags to designate which tape belongs to which week, but the tape drive will not recognise the coloured labels, so using an expiration date for the tape will help preserve that backup until it is time for the tape to be reused as part of the normal cycle.

Of course it is also necessary to train your operators not to arbitrarily respond to backup requests to OVERWRITE tapes, and in fact to check!

/CRC and /GROUP=n

These are output saveset qualifiers. In my experience there is a time to use them, and a time not to use them. When creating an on-disk saveset, then using /NOCRC and /GROUP=0 both saves CPU time calculating the CRC and the XOR data in the (default) 1 in 10 blocks reducing saveset size. Disk writes have some data integrity built in that make the use of these unnecessary.

There is an argument that tape drives provide both CRC and XOR checking. However, unless you use the /VERIFY, I would advise against disabling the writing of group redundancy data and CRC checks. The XOR data is able to recover lost data blocks from tape, and CRC checks validate the data on tape against any corruption. With the default values additional CPU overhead calculates CRC data, and for every 10 blocks (of /BLOCKSIZE) an additional block of XOR data is written to enable recovery of a lost block. The additional tape used and time used could mean the difference between a whole backup being useful, or useless. Unless you are verifying tapes (reading back) then use this qualifier as additional protection.

Tape device write caches and tape streaming

Some tape drive models, those expected to stream data onto the tape incorporate a write cache. You can see this from a SHOW DEVICE / FULL and is enabled at mount time using the /CACHE=TAPE on the MOUNT line. This permits the hardware caches to hopefully reduce the "start-stop" of the tape. Many modern fast streaming tape drives have a write cache that is invisible to the operating system, you only need to enable it if the device shows it. Typically this is older tape devices, the TK70 is one example, but some high speed DDS (DAT) drives also have them.

Tape streaming merely refers to the way a tape is written. All tapes have start and stop blocks with a gap. More on the size of the blocks later, but the objective is to write block after block after block without stopping the tape, this is called tape streaming. Starting and stopping the tape significantly delays the time taken to write any data as the tape has to be in the correct position and at the correct tape speed in order to write (or read) data. The tape drive has to rewind, then wind forward to a particular part of the tape and you can hear or sometimes see tape drives doing just this. A streaming tape drive would sound or look like a tape being slowly rewound or fast forwarded. Comparatively writing the data is far faster than the time to start up or stop and rewind a tape so reducing this effect brings huge elapsed time benefits.

Making BACKUPs quicker

Or more to the point, less elapsed total time. Around version 5.2 of VMS, some significant changes were made to the BACKUP behaviour in order to address performance issued in two areas. Firstly that of fragmented disks, and secondly to buffer the data for better efficiency with the devices concerned. However there is quite a basic way of getting improvement is not already implemented:

/BLOCK_SIZE = 8192, 32256, 65024

This is a save set output qualifier and determines how big a backup data block is. By default (and for generic tape device compatibility) it is 8192, and many installation savesets are written with this size. However as tape blocks are written sequentially, with a gap, causes frequent tape start stop start stop activity. Writing a larger block size of 32256 means that four times the amount of data is written in a single start stop tape operation. This change alone can significantly reduce the elapsed tape writing times without any further modification.

32256 is an important number to OpenVMS in that it is the largest rounded block size that fits with both disks and tapes. Occasionally you may wish to copy a saveset from tape onto disk, and block sizes larger that 32767 cannot be written to a files-11 disk. In my tests using a block size of 65024 gives marginal improvements over 32256 even to SDLT devices and DDS4 devices so the drawback of not being able to copy a saveset to a disk staging area for me tend to outweigh the use of too large a tape block size.

"But my tape is written serpentine!"

Regardless of the underlying technology on tape, it is still a serial access medium, and each track in that serpentine pattern requires an inter block gap. While it is true that the tape is written along its length multiple times, in traditional terms this should be viewed almost as a stack of (reel to reel) tapes, and the overall length of the tape is calculated by the actual length, multiplied by the number of complete written tracks. E.g. if a tape is 500 metres long, and is written to with six tracks* (three forward, three reverse) the total effective tape length is 1500 metres.

*The word 'track' does not represent the standard reel to reel recording technology where bits within the data are written in parallel where each track is a single bit, and the set of tracks make up the data byte.

"But my tape is written helical scan!"

These are the DDS (and 8mm) type technologies that work on the same principle as a video tape recorder. The heads that read and write the data, there are a pair for a single track, are mounted on a spinning drum. The drum is set at an angle to the tape, and the tape is partly wrapped around the spinning head. The relative high speed of the spinning head allows a very high recording density on the tape, actually making a lot of very thin stripes along the length of the slow moving tape. In effect it allows slow tape movement, but keeps the relative speed of the read and write head high.

Each generation of technology (DDS1, DDS2, DDS3 and DDS4, or, Video standard play, long play, etc) represents a higher recording density (narrowly packed data) compared to the total length and tape speed. However the tape is used in one direction only and just once. Nonetheless there are still inter block gaps.

BACKUP software changes and quotas, VMS 5.2, OpenVMS 7.3

As a direct result of 5.2 backup changes, a technical article was published by Digital titled "Backup Tuning" which had a number of recommendations. It had a set of process quotas, and quite importantly ratios of the process quotas, and some SYSGEN settings. The process used the FILLM and respective CHANNELCNT to concurrently open as many files as possible, and the working set quotas to firstly sort the disk reads into a sequential order low to high, and read as much data into memory as possible before performing a continuous write to the tape, to allow it to stream. Later hardware has introduced some interesting side effects mentioned later about IO saturation but first the theory of speeding up your backups. The exact numbers and ratios are ignored here, please refer to the updated article which can be found in the ITRC at HP which is based on "VMS Version 5.2 BACKUP Performance Tuning" and "Setting Up Params For OpenVMS BACKUP Operation (V5.2 and Above)". The former is the reprint of the article discussing changes, the latter some practical advice on setting quotas. The same article does advise that you have a separate account for BACKUP due to the process quotas being used, and that this account will have the capability to saturate your system when running. While this normally results in poor performance for other users, some conditions can cause other issues as noted in a saturation discussion later. The updated articles can be found with a search of "VMS backup tuning" which has modified values for more recent version of Alpha and Itanium OpenVMS.

I will not repeat the details from either article but point out the significance of some items. Firstly the CHANNELCNT SYSGEN parameter on the system governs the maximum number of concurrent file IO channels available to all processes on the system. Large numbers result in a small memory overhead for the process header size but for today's systems with large physical memory this should not be a problem, but be aware that the number of processes present on the system use the same value, so more processes equals more overhead. Next the FILLM which is the corresponding maximum concurrent files that a process may open and should be a maximum of just short of the CHANNELCNT on a system. The two edges to this are that for high values a process can concurrently open many streams to files, but having a value higher than the CHANNELCNT can result in occasional NOIOCHAN errors should a process attempt to exceed CHANNELCNT with too high a FILLM.

In practice [for older systems] the advice is to have a large CHANNELCNT, typically 2047, and a process FILLM of 2000. Be aware of the effects of PQL_DFILLM and PQL_MFILLM the SYSGEN parameters! These figures are lower for more recent versions.

WSQUOTA is a key value that the operating system will grant memory to the value of on the system, and at the cost of other processes if necessary. WSMAX is the biggest physical working set memory size allowed so must be the bigger or equal of the largest WSQUOTA. It is presumed that your backups will take place with little other system activity so causing swapping or paging of processes in physical memory should not be a problem on limited memory systems. If you have active processes requiring memory which causes excessive paging, then bear in mind the IO subsystem of the computer will be more heavily loaded and could adversely affect any expected gains.

DIOLM

This limit the number of concurrent outstanding direct (to device) IO requests that can be “in flight” in an asynchronous data input and output process. This requires memory to buffer each IO as they complete but also gives the process the opportunity to group the IOs so they can be written serially taking advantage of the data grouped for the write operation.

BIOLM and BYTLM

Buffered IO limits the number of concurrent outstanding buffered (via an intermediate IO staging area, e.g. device driver or hardware buffers) similar to the direct IO mentioned above. Buffered IOs tend to have more dependency in their completion are potentially more likely to be delayed as the system has less control over the device concerned, usually because it is not directly attached. Nonpaged pool is used and the size is determined by the process’s BYTLM. The value of BYTLM if too small can reduce the effect of a large FILLM and ratios are discussed in the article.

ASTLM and ENQLM

The outstanding DIOs require a corresponding high ASTLM (asynchronous system trap limit) in order to maintain the high number of outstanding IOs. ENQLM allows the backup process to hold a number of locks on the system.
The advice is to use the ratios and settings relevant for your version of the operating system in use. Be aware that these settings will saturate your system.

Memory quotas, PGFLQUOTA, WSQUOTA, WSEXTENT

Apart from a basic amount of program variables, the prime use of memory is to cache the data, that is, to read in as many files, in name order but from the disk in a sorted, LBN order, into memory, ready to write to the output device (usually tape). Therefore the perfect size would be the size of the disk being backed up, but any figure vaguely in this direction will help! Strictly PGFLQUOTA (i.e. the pagefile) is not generally used for caching data but is required for sorting operations, where SORT makes some basic assumptions about how to perform a sort based on the available virtual memory.

Disk IO saturation problems

While it is a good idea to make your backups complete in as short a time as possible, BACKUP does have the capability to totally saturate the IO subsystem of any computer or connected device. In worst cases devices can go offline or mount verification, and log hardware timing errors, IO stacks can be corrupted, and similarly disks go offline or systems can crash! So to contradict the information above here are a few things to avoid that situation.

What happens is that the process in an attempt to use up all its quotas, will issue read and write requests, and can on occasion exceed the stack space and IO buffer area for the devices. While increasing the stack size (per processor and IO device) can help, a process can still overdrive a device.

Firstly reduce the DIOLM for the process, which may also involve reducing the PQL_MDIOLM value in addition to the UAF record for that username, and potentially the batch queue settings. In many cases if you are seeing problem with backups overloading IO systems, reducing this figure (in a real world example, it was reduced from 2000 down to 20) this had little to no impact on the overall backup completion time.

If problems are still seen, then proportionally reduce the quotas until the backup operation stops impacting normal operation.

Lateral backups!

This is not a method of backing up, so much as an alternative way of doing it. If you have heavily loaded systems, then you may wish to invest in a dedicated backup engine for your system. This is most effective in a cluster environment with shared storage, but you can have a system with multiple dedicated IO cards for tape devices, and do think carefully about the IO paths to the data being read (backed up). If you have a common situation of a CI cluster with the tape drives connected to a HSJ type controller, remember that the data is being read and written over the CI. Using host connected tape devices means that the “write” loading is removed from the shared paths. An understanding of MSCP served disks is helpful in determining the best way to configure a backup engine type system. You may wish to use this system as a “quorum” node in a cluster.

Summary

It is quite easy to make a backup that is totally useless. Always test your backup to the point of restoring the complete disk (as replaced by hardware or purchased brand new). The backup frequency should run with the total amount of data loss you can withstand, and the time to recover the data (after allowing for system rebuild operation). If disaster recovery is a necessary part, ensure that tapes can be properly identified, and a procedure for restoration is in process, a method of booting BACKUP so that necessary tapes and disks can be accessed by the system which is restoring the data. Needless to say, a sound offsite storage and retrieval process is also key and in many cases a legal requirement under Data Protection regulations. Making your backups run faster, take less time and system resources are nice to haves, but need to be balanced between preserving your data, or letting it go extinct.

Nic Clews, CSC Computer Sciences March 2007.
The author can be contacted by email at nic@hpug.org.uk

Are You Getting Enough – HP Interex Newsletter

HP-Interex-EMEA (the co-ordinating body of HP user groups in Europe) publishes a weekly electronic newsletter featuring news about and from HP.

It's a useful complementary publication to ePing. Free subscription is available to all members of HPUG at http://www.hp-interex.com/ulink/

HP-UX Backup

Although Unix has a number of built-in commands to perform backup tasks, they are far too crude to handle the demands of today’s storage requirements. The biggest concern for the administrator is reliability and size of the backup sets. The legacy tools such as tar, cpio and dump cannot handle unlimited file sizes. The limit is 2 Gb per file for these tools or with a patched version of tar, up to 8 Gb for a file. Unfortunately, 2 or 8 Gb is simply too small for today’s systems. Now tar and cpio have one useful feature – they are industry standard formats and can be shared with other non-HP-UX systems. There are also GNU versions of these tools which do not have file size limitations but they use a non-standard format which is incompatible with other systems unless they have the same GNU utilities. So for exchange of data between systems, use the standard HP-UX tar or cpio, and be sure that all files are 2Gb or less in size.

Now there is a much bigger concern with the classic tools – they do not have tape-specific features such as status checking, retries and error recovery. And they do not have a central directory, very important when recovering a specific file and it is unknown whether the files exists on the tape. If a tar or cpio tape takes 2 hours to complete, getting an index or table of contents will require 2 hours to create as the entire tape must be read. None of the legacy Unix tools have a central directory or tape handling.

Another requirement for modern system backups is the ability to identify the tape even if the paper label is removed or was never updated. A reliable backup tool will not only identify the date and scope of the backup but will also identify the tape number for multi-tape backups. Tar, cpio, dump, etc cannot handle multi-tape backups which also limits their usefulness for large backup sets. Another reliability requirement is to prevent appending additional backups on the same tape. While system administrators have done this for years, these are time-bombs waiting to lose valuable data, whether it is due to incorrect positioning of the tape before appending, or loss of records concerning what backups are actually on the tape. The savings in extra tapes is false economy when the data cannot be recovered.

With large data sets (hundreds to thousands of gigabytes), a single tape is not adequate although the newest Ultrium drives can indeed store several hundred gigabytes. But this storage comes at a very steep price. The design of all modern tape drives, starting with the DDS (also known incorrectly as DAT) drive, are known as streamers. That means that they cannot start or stop quickly like the legacy ½" reel-to-reel tape drives. So the data must arrive at the tape faster than the tape runs, and with the latest generation Ultrium (LTO), this exceeds most network connections. Indeed, even some disk drives cannot keep up with the Ultrium 960 which requires more than 120 Mb/sec to run at full speed with 2:1 compressible data. So putting a higher capacity tape drive on an older (slower) system will severely degrade performance in many cases. The reason is that once a streaming tape drive runs out of data (starvation), it must stop, backup into the previous record areas, wait for more data, then take a running start to get up to speed and start recording at the right spot. During this 3-5 second delay, the throughput is zero!

Note also that networks are EXTREMELY slow for modern tape drives, too slow in most cases without the use of parallel LAN connections, also known as teaming or port aggregation. Here is a table of typical throughput for popular LAN speeds:

LAN Speed (bits/sec)	***Throughput (bytes/sec)***
10 Base	**800 Kb/sec**
100 Base	**8 Kb/sec**
1000 Base	**80 Kb/sec**

The table calculates the byte rate by dividing the bit rate by 10 (8 bits/byte plus overhead), then uses 80% for the useful rate on a switch (much less with hubs and shared traffic). So a typical 100 Base LAN cable is too slow for most modern tape drives and the throughput will be much less than rated speed due to streaming dropouts. The following table shows the required speeds for various tape drives. HP's Ultrium drives also have a feature called Adaptive Tape Speed (ATS) or Data Rate Matching (DRM), which matches the speed of the tape to the data rate of the server. It is fully variable between its lowest and highest rates and eliminates tape repositions within this range - thus reducing wear even if the server cannot keep up.

Tape drive	**Lowest native data rate**	**Highest native data rate**	**Highest rate with 2:1 compression**
HP DAT 24	n/a	1 MB/Sec - 60 MB/min	120 MB/min
HP DAT 40	n/a	3 MB/Sec - 180 MB/min	360 MB/min
HP DAT 72	n/a	3 MB/Sec - 180 MB/min	360 MB/min
HP DLT VS80	n/a	3 MB/Sec - 180 MB/min	See note below
HP DLT 80	n/a	6 MB/Sec - 360 MB/min	See note below
HP DLT	n/a	8 MB/Sec - 480 MB/min	See note below

Tape drive	Lowest native data rate	Highest native data rate	Highest rate with 2:1 compression
VS160			
HP SDLT 220	n/a	11 MB/Sec - 660 MB/min	1320 MB/min
HP SDLT 320	n/a	16 MB/Sec - 960 MB/min	1920 MB/min
HP SDLT 600	n/a	36 MB/Sec - 1920 MB/min (1.92 GB/min)	3840 MB/min
HP AIT 70	n/a	4 MB/Sec - 240 MB/min	480 MB/min
HP AIT 100	n/a	6 MB/Sec - 360 MB/min	720 MB/min
HP AIT 200	n/a	12 MB/Sec - 720 MB/min	1440 MB/min
HP Ultrium 215	6 MB/Sec	7.5 MB/Sec - 450 MB/min	900 MB/min
HP Ultrium 230	6 MB/Sec	15 MB/Sec - 900 MB/min	1800 MB/min
HP Ultrium 232	10 MB/Sec	16 MB/Sec - 960 MB/min	1920 MB/min
HP Ultrium 448	10 MB/Sec	24 MB/Sec – 1440 MB/min (1.4 GB/min)	2880 MB/min
HP Ultrium 460	10 MB/Sec	30 MB/Sec - 1800 MB/min (1.8 GB/Min)	3600 MB/min
HP Ultrium 960	27 MB/Sec	80 MB/Sec – 4800 MB/min (4.8GB/min)	9600 MB/min

So DDS drives are OK for 100 Base LAN connections but all other drives have much higher speed requirements. Note that when the tape drive is compressing the data, perhaps as much as 2:1, the MINIMUM data rate is twice the native data rate. Again, if the link (and/or computer and disks) cannot keep up, the drive will stop/restart excessively and reduce the throughput by 5:1 to as little as 100:1, while drastically increasing wear on the tape and drive.

Now if the link speed is adequate, the next concern for modern tape drives is the speed at which data can be retrieved from the filesystem. Note that raw volumes do not have the overhead of directory structures and files, but tools like tar and cpio cannot handle raw volumes. The worst scenario for file backup is thousands to millions of files less than a megabyte. The reason is that it may take longer to find, open, and read the file than it takes to write the data on the tape. Single threaded backup tools must do everything one at a time. Modern backup tools will run several threads or sub-processes to fetch the data and keep the data stream running at maximum speed.

Most commercial backup tools do indeed run multiple file readers as well as provide a central index and error recovery. While these can be expensive, the value of the data is always the overriding metric. Like cheap insurance for an expensive building, it will be of no value if it will not pay off when it is needed. So too are free or cheap backup tools which seem to work OK but the tapes either do not contain the expected data, or data errors prevent recovery.

An exception to the free-opr-cheap rule is fbackup, the native HP-UX backup tool. It has no file size limitations, will start as many as 6 file readers, provides a central index on every tape, and handles multi-tape backups. In fact, each tape from a multi-tape backup has the complete index for the job as well as the tape number and date, all immediately readable. Unlike tar, cpio or dump, frecover can read and display the entire table of contents in just a few seconds from any tape in the backup set. And unlike legacy tools, frecover can make use of special tape codes (search marks) that are recorded by fbackup to aid in high speed positioning. Rather than wait for two hours to get one file at the end of the tape, frecover can position the tape at high speed, taking only a couple of minutes to reach the end of the tape.

Fbackup can run a script at the end of the tape that changes tapes in an autochanger or tape silo. Scripts would use the mc command to read the contents of the silo (using the tape media barcodes) and pick the correct next tape to use. Fbackup prevents accidental overwrite of a previous tape in a multi-tape backup by checking the new tape's label. Fbackup can also backup to a remote system although throughput is limited by the LAN connection, and since fbackup does not have direct control of the tape drive, highspeed search marks cannot be written. Such network connections are limited to other HP-UX systems as fbackup is a proprietary tool.

Frecover also has the ability to recover from tape errors and can be restarted in the middle of a long restore process. When restoring a file from a multi-tape backup, you can put the last tape of the backup in the drive, run frecover and it will tell which tape contains the file that you want.

When using fbackup, a config file is ALWAYS required. The defaults for fbackup are designed for ½" reel-to-reel magtape and are inefficient for DDS, DLT and other modern tape drives. The following file should be used for all fbackup runs:

```
blocksperrecord 4096
records 64
checkpointfreq 4096
readerprocesses 6
maxretries 5
retrylimit 5000000
maxvoluses 200
filesperfsm 2000
```

The parameters are:

```
blocksperrecord 4096 (for better tape utilization)
records 64 (shared memory records)
checkpointfreq 4096 (records between checkpoints for recovery)
readerprocesses 6 (parallel processes to read file data)
maxretries 5 (times to retry reading a locked file)
retrylimit 5000000 (5 Megs max retry space)
maxvoluses 200 (times to reuse the same tape)
filespersm 2000 (files between search marks)
```

Other parameters are:

```
chgvol <filename> (script/program to run at end of tape)
error <filename> (script/program to run with fatal errors)
```

Fbackup understands tape drivers and must be updated for newer drives. This means that unsupported versions of HP-UX such as 10.20 will not be compatible with new drives such the Ultrium 960. Even if it were to work, the computers that run 10.20 are far too slow to keep this drive busy so performance will be quite poor.

Fbackup can save files to tape, or a remote tape on another HP-UX system (remsh is required for this to work), or save to a file or pipe. Here are a few examples using fbackup and frecover:

```
fbackup -i / -v -c config-file -f /dev/rmt/0m
```

The –i option specifies inclusion, -e for exclusion and there is no limit on the number of –i and –e options on the command line. They are processed left to right so you can include / then exclude /dev.

An alternative for a complex list is to use a graph file (-g) which has one or many “i” and “e” lines.

Display the tape header with dates:

```
frecover -V - -f /dev/rmt/0m
```

Display the table of contents:

```
frecover -I - -f /dev/rmt/0m
```

The man page for fbackup and frecover covers the option in more depth.

File Area Networking – Josua Braun, Brocade

In the nineties, IT managers began to realize that the DAS model (Direct Attached Storage) was not anymore sufficiently scalable: performing tasks such as management, backup and consolidation was just too complex and time consuming in most environments, because all these tasks needed to be performed on a per server-storage basis. The SAN (Storage Area Network) was the breakthrough technology designed to overcome the limitations of the DAS model. By allowing servers to access their storage device via a Fibre Channel or IP network (FibreChannel or iSCSI), the SAN enables the abstraction of information like physical locations and parameters of the disc, from the server file system logic.

With SAN technology, storage administrators can centrally manage and consolidate data, thus giving them the ability to perform tasks such as backup, capacity extension and high availability, from a central location. Virtualization of volumes was a major step for storage administrators. Nevertheless, there is still a one-to-one relationship between the server (SAN initiator) and the volume (or LUN, SAN device).

Therefore, this model is the optimum solution for high-performance applications running on servers that require direct control over the file system (like high transaction databases for instance), and need access to structured data (block level).

Today, companies face similar management issues in the world of unstructured file data as they saw 10 years ago in block-level storage. Distributed mass storage systems become more and more of a nightmare in many organizations, and they are seeking for a cost-efficient, scalable and future proof management technology. Emerging technologies are on the way to address these problems.

This article will describe the functionality of those technology approaches and show how the well known benefits of SAN can be realized in the world of file data. With unstructured data, the technical approach is different: A virtualization layer needs to be added between the server (connected to its storage), and the client (user or application server), since they cannot access the server data at the block level. The two common standards that are used today to provide this access layer are IP based protocols such as CIFS (common internet file system) for Windows environments and NFS (network file system) for Unix environments. Via those protocols, storage clients can access files (unstructured data) by sending requests to the CIFS or NFS layer of a storage server. The main difference between a storage server (SAN-attached server for instance) and a NAS device (Network attached storage), is that the NAS operating system is a simplified OS (when compared to standard windows/Unix Os) whose main purpose is to share files through CIFS and NFS (even tough some NAS can provide Fiber Channel or iSCSI volumes as well, in which case they behave just like standard SAN storage devices).

By shifting from DAS to SAN, storage administrators were able to virtualize volumes, thus getting rid of the physical dependency between the server and its storage. Using CIFS or NFS on storage servers allowed them to let several end-clients access unstructured data (files), regardless of the physical storage layer. But at the end of the day, end clients were still accessing files by requesting a specific server: the physical dependency had moved from physical mapping of the server-storage to physical mapping of the client-server connection.

In a simple environment, based on a single file server, this storage client-file server dependency can still be handled without excessive management. In a more complex storage environment with multiple file servers, however, the management effort soon reaches a critical limit. The number of storage client-file server relationships will increase at least up to the number of file servers. In this case, many seemingly simple but important tasks such as moving data across file servers, making them highly-available or tiering the storage architecture, will have an impact on several thousand client-file server relationships.

To handle these multiple relationships more efficiently while minimizing impact and downtime for end-clients, a new virtualization layer is needed: this is exactly where the FAN comes in.

As stated by IT analysts such as the Taneja Group or IDC, the FAN (or File Area Networking), is a combination of software and hardware technologies, whose main purpose is to organize, route, manage and provide consistent access to file level information available in the storage network.

Among the many benefits of the FAN model are:

- The ability to manage the data according to their business value, no matter what platform they are physically stored on (one benefit of the file-level data compared to the block-level data),
- The capacity to manage and display file views to users based on access rights or organizational information (such as project, department, sites…)
- The functionality to migrate file information across storage platforms in the most transparent and least disruptive way for users, and, finally
- The aptitude to look at the file information sharing in a service-oriented way: the FAN is a way to provide every user access to the file information they need throughout the company - regardless of their location or the physical nature of the storage platform.

To better understand the functionality and benefits of FAN, below is a description of the six layers that constitute a FAN (as defined by Taneja Group), and the important elements that need to be considered about them:

The storage devices are the basic level on which other FAN layers are based on. Any device, from a SAN attached server to a NAS appliance, even a simple server with embedded disks, could be considered as a FAN storage device. The only prerequisite is that the FAN storage device´s shared files resources can be accessed by end clients over the network.

The second layer is the file serving device: it plays the gateway role, in order to let end users access FAN storage device file resources via the IP network This interface can be either embedded in the FAN storage device itself (in case of a NAS device for instance) or exist on top of a server OS connected to a SAN storage (or DAS storage). Any FAN storage device must have a file serving interface compliant with standards file sharing protocols such as CIFS (Windows) and NFS (Unix).

In the FAN model, the combination of storage device and file serving interface is abstracted from the storage client view, since end clients are mostly accessing FAN file resources through CIFS or NFS requests.

Nevertheless, in order to provide more advanced FAN features such as file-based data movement or archival policies (e.g Information Lifecycle Management), some support of the storage device operating system (like dedicated storage OS on NAS appliances) may be needed to achieve better efficiency.

To put it simply, the first and second layers of the FAN model (storage device and file serving device) are abstracted from the third layer that is described below, namely the namespace layer. The namespace layer is the core of the FAN model, providing the virtualization necessary for all functionalities that a FAN enables. There are several types of namespaces, ranging from non-shared and shared namespace, to global namespace, and all of them share the same capabilities: being able to collect, organize and present file-level information to authorized end-clients, regardless of their physical location.

Since the namespace layer is the core layer in the FAN model, it is important to avoid making it a single point of failure. This is the reason why the global namespace is the most secure: with a global namespace, the namespace layer is used only as a directory for file-level resources, and provides the physical referrals to these resources as soon as a user requests a file. The core functionality is best compared to the functionality of a DNS server: requests for physical resources are being realized via aliases, and then the global namespace establishes the physical connections between the end client and the physical resource. In an Out-of-Band global namespace solution, this prevents the global namespace from becoming a bottleneck (from a IOs point of view). Also, as the namespace information has been cached on the client, the client can continue working on his file resources even in case of a namespace outage.

Despite this inherent high availability, in order to take full advantage of the FAN features - like the ability to move data across storage devices with minimum impact on end clients – the global namespace layer should be made highly available e.g. by clustering of the namespace servers.

The fourth layer of the FAN model, namely the file management and control services, are best described as the intelligence layer. All these services interoperate with the global namespace: doing migration in the FAN model would e.g. dynamically update all obsolete references with new ones, in order to redirect users to the correct file resource; replication can be associated with target-based failover policies, and the FAN solution has the ability to monitor the validity of these targets at any time, thus automating the failover process in case of primary target failure; criteria-based classification policies can be used to have a better grasp of what type of data is stored within the storage devices; load-balancing shares, together with the global namespace update, data among several storage devices while minimizing the data movement impact on end users; namespace-based logical views can be generated by crossing over information related to user accounts and their access rights on storage resources; retention in the FAN model, once automated by rule-based archival and restore policies, allow storage administrators to deploy hierarchical storage management (or ILM) to get better ROI from their investment in high-end storage devices.

At the core of every FAN implementation is – apart from the global namespace such as Windows DFS – an intelligent and efficient management layer. i.e. a set of tools for FAN management, administration and monitoring such as the FAN portfolio from Brocade. These solutions allow for efficient setup and management of the namespace as well as provide the management and control services as described as the "fourth layer" of the FAN.

The fifth layer is the connectivity one; as we explained before, in the FAN model users can access the file information regardless their own location, and the physical location of the data itself. That means clients should be able to access their data, being connected to the FAN infrastructure through local or distant network connection (LAN or WAN connection). In order to minimize performance differences between these two access modes, technologies such as wide-area services (WAFS) and file data over wan optimization may be used. The main purpose of the connectivity layer for the FAN model is to cope with heterogeneous network connections, without impacting user performance feedback; this element needs to be considered if the FAN has to be deployed in central-remote sites environments.

The end clients are the sixth layer of the FAN model; any client machine that can access its data via the FAN namespace is a FAN end client, which virtually means that any platform able to request files through CIFS and/or NFS protocols, is eligible for FAN.

All these layers on the FAN model finally have the same purpose: provide consistent access to file information. All traditional storage management tasks can then take advantage of the FAN.

Migrating file data across local or remotes storage devices, consolidating data from several smaller storage devices to a central storage repository, are common tasks that can be optimized by the use of FAN global namespace technologies. Having a centralized view of all data resources across multiple locations is critical to the storage administrator, because it allows him to optimize use of existing storage devices, and present them to end users in a more logical and efficient way.

Security and compliance aspects are also critical for FAN architecture: showing storage clients a logical view based only on the resources they have access rights to, regardless of their physical location, is a sweet point for any compliance driven storage infrastructure.

Moving data with minimum impact on the way users are accessing it is a key element of the FAN model, especially if migration is performed via automated, criteria-based policies. If data can be moved without preventing users from accessing it the way they were doing it before, the concept of hierarchical storage management (or information lifecycle management) can be used seamlessly within the storage environment. The data life cycle management can be simplified by the FAN tiered approach, and allow storage administrators to improve use of high-end storage, while minimizing backup time on the more active, highly-available storage devices.

Once the file data has been consolidated and made easily accessible through the FAN namespace layer, it is also significant to automate all business continuity/disaster recovery/failover polices on the consolidated storage devices. This can rely on backup and restore policies, and most likely in FAN on replication policies between storage devices. Once a file resource is synchronized across several depositories, a disaster recovery policy can be associated to link all these repositories together, and eventually monitor and update the namespace target validity in case of loss of one of the resources. This example outlines the fact that the monitoring and update of the namespace layer is a key point of the FAN model: when a resource is virtualized, targeting the most relevant one is essential.

With File Area Networking, a lot of network challenges can be solved. The virtualization of file storage plus the additional management and control services as well as extension of this functionality across geographical borders make the administrator´s life much easier, as they enable independent scaling and managing of the logical and the physical storage layer on a global level. For organizations with more and more complex storage systems for their unstructured data, FAN is a key element of a future proof management structure with reasonable storage TCO and scalability for future challenges and growth.

CONNX Solutions Announces Continued Commitment to OpenVMS on HP Integrity Servers

Redmond, Washington, 15 February 2007

CONNX Solutions, Inc., a leading provider of simplified data access management and integration software solutions, announced today that in Q.2, 2007, it will offer Oracle Rdb and Codasyl DBMS support for OpenVMS on HP Integrity Servers. CONNX Solutions currently supports RMS and Oracle on the same platform.

Customers using CONNX for RMS on HP Integrity servers running OpenVMS have reported a significant performance increase - two to three times faster than RMS running on Alpha Servers - and customers using CONNX for Oracle Rdb and Codasyl DBMS on HP Integrity servers running OpenVMS should experience a similar increase in performance. CONNX Solutions began offering RMS support on HP Integrity Servers running OpenVMS in April 2005.

“We are committed to supporting the HP Integrity platform with all related data sources and are pleased that customers are satisfied with the performance gains of using our products on this platform,” says Larry McGhaw, the CTO & VP of Engineering at CONNX Solutions.

With the addition of Oracle Rdb and Codasyl DBMS support on HP Integrity servers running OpenVMS, Enterprise businesses can transition to a higher performance platform.

Currently CONNX for RMS and Oracle on HP Integrity servers running OpenVMS provides secure, real-time, read/write SQL access to those databases and allows database users to perform seamless joins between RMS, Oracle and most other legacy and non-legacy databases. In Q.2, 2007, CONNX for Oracle Rdb and Codasyl DBMS on HP Integrity servers running OpenVMS will provide real-time, read/write SQL access to Oracle Rdb and Codasyl DBMS and allow seamless joins to be performed between Oracle Rdb, Oracle Codasyl DBMS and most other legacy and non-legacy databases too.

CONNX for RMS and Oracle on HP Integrity servers running OpenVMS is currently available for purchase. You can purchase CONNX for Oracle Rdb and Codasyl DBMS in the second quarter of 2007. Contact Generix Limited on +44 (0)1924 500151 for pricing information.

“Today’s data centers increasingly rely on secure and easy access to management applications,” said Michelle Weiss, vice president of marketing, Business Critical Systems, HP. “The availability of CONNX solutions on HP Integrity servers running OpenVMS ensures our loyal customer base can maximize their investment while simplifying IT operations.”

About CONNX Solutions

CONNX Solutions, located in Redmond, WA, is a leading provider of simplified data access management and integration software solutions that allows users to directly access and manage vital enterprise information from more than 40 data sources including Adabas, RMS, Oracle Rdb, Oracle Codasyl DBMS, Oracle, DB2, SQL Server, Sybase, Informix, C-ISAM, D-ISAM, Micro Focus, VSAM, IMS and DataFlex/Powerflex databases.

CONNX, DataSync or InfoNaut have been used by over 3,000 organizations worldwide. CONNX is relied on by government and business entities in a wide range of industries, including manufacturing, healthcare, financial services, telecommunications, aerospace, and information technology.

Generix Limited based in the UK is the CONNX European Distributor. Generix have represented CONNX for over 12 years and are a well established HP Business Partner.

Apart from involvement with hpUG the UK HP User Group, Generix are also exhibiting at the forthcoming DECUS **event in Nurnberg, Germany on 16th-19th April**.

"This emphasizes the importance we place on the existing HP user base for our future." stated Leonard Klejnow, Business Development Director, "It is on joint interest that customers continue to use and add to their investment in HP technologies."

Klejnow continued "We believe we can assist HP customers to derive even greater benefits from their HP investments by unlocking their data and allowing them to leverage more appropriate information without embarking on high risk and expensive strategies. Many customers have now built on the reliability of their HP platforms by adding CONNX to deliver the current and future business needs."

A View on HP's acquisition of PolyServe

Sent: 05 March 2007 18:53
Source - InfoWorld

The two companies have been partners for quite some time, and there was a "high degree of potential synergy" between their offerings. I don't particularly like that expression, but if there was ever a slam dunk in this business, HP buying PolyServe was one.

Here's why: PolyServe creates a powerful software bridge between servers and storage, essentially giving business applications and file servers fast, parallel data transfers and the potential to crank up performance and resilience on demand.

Why is this important for HP? Because HP has an insatiable appetite for new customer wins or repeat sales on both ends of that server-storage bridge. If you've been watching the same movie as I have, you'll agree that there has been little synergy between those two powerful groups (servers and storage) inside HP.

Take, for example, NAS systems, which are a typical confluence point of servers and storage devices; they also create opportunities for joint purchase orders. For several years, HP has been quite successful in combining a joint offering of storage systems and servers topped by the Microsoft Windows Storage Server.

Despite that success, the glue to put together those systems – the Microsoft OS -- came from outside HP. PolyServe creates a similar type of bond between servers and storage devices, promising an appealing level of performance and resilience.

PolyServe's customer roster already contains a wide range of vertical markets. That's because PolyServe is basically an HPC (high-performance computing) solution that business customers can deploy and manage without putting too much stress on their IT structure or their staff. With PolyServe, customers get the extra performance required by, say, the deluge of multimedia files common to every business sector and can keep using their same servers and ...

More of this column at:

http://newsletter.infoworld.com/t?ctl=16842C7:9107B0F8CA93EBA2F8DADA5E6BD4BA2EEFF29049075316B4

[mailto:storageinsider@newsletter.infoworld.com]

Can HP Fool Moore's Law? By Michael Kanellos

How do you make chips more powerful? Take stuff out, according to a new proposal from Hewlett-Packard.

Researchers from HP Labs plan to publish a paper this month that outlines how it may become possible to substantially increase the performance of certain types of chips, and reduce their power consumption, by replacing the communication wires inside chips with an overhead grid of tiny nanowires.

The architectural concept could prove a novel way to help tackle one of the major problems facing semiconductor designers -- how to continue to shrink chips and the components inside chips.

For full story see: http://news.com.com/2102-1008_3-6150057.html?tag=st.util.print

OpenVMS Backup Products: ABS/MDMS and Data Protector Compared by Ted Saul, Technology Consultant

Source - OpenVMS.org News 28 Jan 2007

Overview:

HP offers two backup applications for the OpenVMS operating system at this time: the Archive Backup System/Media and Device Management Services (ABS/MDMS) application and the Data Protector application. This article will point out the similarities and differences between the two, in order to help in the selection process between the products. There are also other backup applications from third-party vendors but this article will not cover them.

ABS/MDMS has been the go-forward application of choice for OpenVMS for a number of years. Development of ABS/MDMS has included new functionality as well as support for the latest devices and operating system releases. HP has also been developing the Data Protector product for many years as well. Formerly known as Omniback, this product is not OpenVMS-centric. It was developed for the large enterprise where multiple operating systems are deployed along with a Storage Area Network (SAN), direct accessible, or network tape devices.

Full Article: http://h71000.www7.hp.com/openvms/journal/v9/abs-dataprotector_differences.pdf

OpenVMS to Support HP BladeSystems c-Class

HP OpenVMS is pleased to announce that in June 2007, with the addition of a patch kit based on version 8.3, the OpenVMS operating system will support HP BladeSystems c-Class (BL860c). The HP BladeSystem c-Class was designed from the ground up to deliver the future of scalable infrastructure design today - a clean-slate design and significant leap forward.

The HP BladeSystem c-Class portfolio takes advantage of the best technologies across HP and brings them together to fundamentally improve how customers buy, manage and use their computing resources. HP BladeSystem c-Class infrastructure offers flexibility and scalability by allowing customers to manage server, storage, networking and power management as a unified environment.

HP Integrity servers are now available in BladeSystem c-Class

Now, for the first time in c-Class, customers can employ the benefits of Integrity servers in a BladeSystem environment. The BL860c features support for all four Integrity operating environments; HP-UX 11i, OpenVMS, Windows and Linux – both Red Hat and SUSE – and Windows 32/64. (Windows support is scheduled for 2H 2007.)

By supporting Proliant server blades in the same enclosure customers have the dual benefits of Integrity and Proliant applications running in the same enclosure. By year-end 2007 OpenVMS will support common Blades Management with HP-UX, Linux and Windows, easing provisioning and administration of multiple operating systems in the common chassis.

Up to 8 separate instances of OpenVMS can be deployed in one BladeSystem c-Class enclosure, enabling different versions of OpenVMS and different tasks (development, support, production, testing etc) to be isolated from each other if required.

How Blades Enhance attractiveness of OpenVMS

{mosimage}

- Up to 8 seperate instances of OpenVMS 8.3-1H1 and subsequent versions sharing the 32 cores
- Save multiple OpenVMS environments on the SAN
- Even use *Backup* to save and restore different environments

Benefits:

- Pure OpenVMS environment and commands
- High performance - native, direct I/O
- Seperate support, production, test and development environments all possible in one chassis if required
- Inherent compactness and environmental advantages (power, cooling, footprint, etc) of Blades

The BL860c Server Blade is a key member of the BladeSystem c-Class family

The BL860c is a 2-socket, full-height, c-Class server blade featuring single- and dual-core Itanium® 2 Montecito processors. It supports up to 48GB of memory in 12 DIMM slots and utilizes the HP zx2 chipset. Up to 8 BL860c servers can populate a single c-Class enclosure and 32 BL860c servers can be configured into a single rack for compelling server density.

The BL860c features up to 2 internal SAS small-form-factor hard disk drives, 4 embedded Gbit LAN ports as well as 3 mezzanine cards for a wide range of I/O support including fibre channel and InfiniBand fabrics. The hard disk drives and mezzanine cards are the same HDDs and I/O cards utilized by BladeSystem c-Class ProLiant server blades. BL860c server blades can be configured along side other ProLiant server blades and HP storage blades in a single enclosure.

For more information go to:

http://h71000.www7.hp.com/openvms/cclass_support.html

US Changes to Daylight Savings

HP has set up a web site that consolidates all the information about the DST change.

It not only has information about how this affects HP products, but has links to all the major vendors' sites regarding the DST changes (kudos to HP for putting this together).

http://h10072.www1.hp.com/dst/

Hints and Tips

HP-UX - How can I restore files or directories from an Ignite-UX archive created with 'tar'

PROBLEM:

Many times a system administrator needs to restore items from a tape, but not to overwrite the existing files. This allows the system administrator to review the restored files.

The following solution details how to save test files using the 'tar' command and to restore those files from the archive to a relative location, using the 'pax' command.

RESOLUTION:

The basic steps for creating an archive using the 'tar' command and restoring files from the archive using the 'pax' command as follows:

Create the example directories
Create the example test files using the '/usr/bin/touch' command
Create the archive using the '/usr/bin/tar' command

Change to the restore directory location
Restore the files from the archive using the '/usr/bin/pax' command
Review the newly created directory and files
Restore specific directories and files from an archive
Restore specific directories and files from a tape archive
Additional information sources

1. Create directories using the 'mkdir' command.

```
  # /usr/bin/mkdir /tmp/restoredir

  # /usr/bin/mkdir /tmp/level2
```

2. Create the test files using the 'touch'command.

```
  # /usr/bin/touch /tmp/file1

  # /usr/bin/touch /tmp/file2

  # /usr/bin/touch /tmp/level2/file3

  # /usr/bin/touch /tmp/level2/file4
```

3. Create the archive with the test files and directories included in the archive. In this case the archive is located in the /tmp directory but could also be located on tape.

```
  # /usr/bin/tar -cvf /tmp/myarchive /tmp/file1 /tmp/file2 /tmp/level2

 a /tmp/file1 1 blocks

 a /tmp/file2 1 blocks

 a /tmp/level2/file3 1 blocks

 a /tmp/level2/file4 1 blocks
```

The above 'tar' command created an archive with absolute path names for /tmp/file1, /tmp/file2, /tmp/level2/file3 and /tmp/level2/file4.

4. Change to the restore directory location (/tmp/restoredir)

```
  # /usr/bin/cd /tmp/restoredir
```

5. Restore the files from the archive using the'pax' command to remove the absolute path identifier.

```
  # /usr/bin/pax -r -pm -s%/tmp/*%% -f /tmp/myarchive
```

The above 'pax' command will restore 'file1' and 'file2', create the directory '/tmp/level2' and restore files 'level2/file3' and 'level2/file4' into the directory /tmp/restoredir.

6. Review the newly created directory and files.

```
  # /usr/bin/ll -R /tmp/restoredir
```

ftp://ftp.hp.com/pub/enterprise/programming_code/c00833216_New_Directory.txt

Click here to see the newly created directory and files

7. Restore specific directores and files from an archive by using the 'pax'command

```
  # /usr/bin/cd /tmp/restoredir
```

Restore just the files in the /tmp/level2 directory

```
  # /usr/bin/pax -r -pm -s%/tmp/level2/*%% -f /tmp/myarchive

 a /tmp/level2/file4 1 blocks

 a /tmp/level2/file3 1 blocks
```

8. Restore specific directores and files from a tape archive by using the '/pax'command

```
  # /usr/bin/cd /tmp/restoredir

  # /usr/bin/pax -r -pm -s%/tmp/level2/*%% -f /dev/rmt/0m

 a /tmp/level2/file4 1 blocks

 a /tmp/level2/file3 1 blocks
```

9. Additional information can be found in the following man pages:

```
  # man pax

  # man tar

  # man mkdir

  # man chdir

  # man touch
```

HP-UX 11.x Operating Environments - tar Commands Hang issue

It was noticed that backups using tar were failing. There were many pending tar commands in the ps –ef output. The tar command hang could be replicated with this simple tar statement:

```
$ tar cf - / | tar tvf -
```

The resulting process could not be killed.

The hang would not occur at the same file, but usually just in vg00 filesystems. No errors or complaints in the syslog.log or dmesg.

SOLUTION:

Check the following:

that current tar patches are installed

that ioscan sees the device
the syslog.log and dmesg for any complaints
try writing to the drive with another command

Tried to backup using another utility, like an Ignite backup (make_tape_recovery command) to see if the same hang occurs with pax (pax is the utility that Ignite makes use of) and to test writing to the tape drive.

It was found that pax was already running and it looked like an Ignite hung from an earlier date, which was about the same time as the backup failures...

It is suspected that the hang was on the tape hardware, resulting in the commands not responding. In order to release the hung processes (tar and pax) the server had to be re-booted; there is no other way to kill a hung process.

HP-UX - Block device versus raw device performance

From time to time, someone will do a dd(1) to a block device and compare the results to a dd(1) to a raw device. To their surprise, the block device will perform much more slowly than the raw device. This article will explain the differences in the results.

The example times below were taken on a K460 using a JBOD disk. The actual speed is not as important as the comparative times between the tests. The dd(1) utility was used to perform the tests using a dd block size of 1024 KB to read or write 100 MB of data to the device.

Operation	device	wall time (secs)
read	raw	15.06
read	block	20.60
write	raw	18.40
write	block	442.58

There are several factors to keep in mind when performing a dd(1) to the devices:

1. Note that in each case, there is no filesystem involved. The dd(1) is performed to the raw or block device (/dev/rdsk or /dev/dsk). Since there is no filesystem involved, there is no readahead. Each read is synchronous. For raw devices, the writes must be synchronous, but for block devices, they are asynchronous.

2. Also, there is no merging of buffers. Typically, buffers are chained together by the filesystem and the volume management layer will merge the buffers when the last buffer in the chain is received from the filesystem. A filesystem, however, is not in use here, so buffers are not chained together and thus are not merged for larger I/Os.

3. Buffers used by the block device are either 4 or 8 KB in size. Originally, the buffers were 4 KB in size, but the recent HP-UX 11.11 patch [PHKL_30992/PACHRDME/English] has increased the block device buffer size to 8 KB. HP-UX 11.23 and above also uses 8 KB buffers for the block device. Since the buffers are not merged, the physical I/O size will be the same size as the buffer size.

4. For raw disk devices, the largest physical I/O is either 256 KB or 1 MB, depending on the driver and operating system. In the test cases above, the I/O size for the raw device was 256 KB.

5. When writing to a block device, a read of each buffer must be performed first, then the buffer is written asynchronously with the new data.

6. The writing of data to a block device is asynchronous. The buffers for writes can consume a large portion of the buffer cache and can cause long I/O queues to the device. Also, when the last close of a block device occurs, all the buffers for the device must be flushed to disk and invalidated. This can consume a lot of CPU time for systems with a large buffer cache.

Given the above factors, we can make the following conclusions:

o Reading the raw device is faster than reading the block device because the raw device is able to issue 4 256 KB synchronous reads for each 1024 KB of data, whereas the block device must perform 256 4 KB synchronous reads (or 128 8 KB synchronous reads depending on the patch level).

o Writing the raw device is faster than writing the block device, in part due to the same reason that reading is faster. However, block writes must read from the device before the data is written. Not only does this cause additional overhead due to the fact that there are twice as many I/O operations, but this read-then-write pattern also causes much more head movement which results in longer I/O service times for the I/O. This may not be as prominent on intelligent disk arrays as it is on the simple JBOD disks as used in this example.

Overall, performing dd(1) tests on a block device is not a very good metric for identifying the actual performance of the device.

Due to all the factors mentioned above, it is not recommended to do dd(1) testing on a disk or volume block device.

Instructions to install the OVPI Sybase EBF 9936

PROBLEM:

On HP-UX systems, srvbuild will not run unless EBF 9936 has been applied. Srvbuild is a Sybase utility that creates new Sybase server instances. Without srvbuild, a backup server cannot be created for Sybase. Without a backup, server backups cannot be performed on any Sybase database. HP ships EBF 9936 on a separate disk for HP-UX versions of OVPI, but this disk does not contain instructions on how to apply EBF 9936.

CONFIGURATION
Operating System - HP-UX
Version - 5.1
Product - performance insight

RESOLUTION:

To apply EBF 9936:

1. Stop trendtimer.

2. Create a backup of the $SYBASE directory.

3. As the superuser create a mount point for the CD-ROM:

```
mkdir  /cdrom
```

4. Use the following command to find the CD-ROM device file:

```
ioscan  -fnC  disk
```

5. Mount the HP OpenView Performance Insight Sybase EBF CD-ROM:

```
mount  -F  cdfs  -o  ro  /dev/dsk/c1t2d0  /cdrom
```

Please note that the /dev/dsk/clt2d0 is the CD-ROM device file and will be different on different machines. It is used here for illustrative purposes only. If you have problems contact your HP-UX administrator.

6. As the sybase operating system user, do a recursive copy from the /cdrom/hpux/ebf9936 directory to the $SYBASE directory:

```
cp  -R  /cdrom/hpux/ebf9936/*  $SYBASE
```

7. As the sybase operating system user, log into the SYBASE SQL server and stop the Sybase SQL server:

```
isql  -Usa  -P<password>

1> shutdown
2> go
```

8. As the sybase OS user, restart the Sybase SQL server:

```
$SYBASE/install/startserver  -f   $SYBASE/install/RUN_<HOSTNAME>_SYBASE
```

When the line "Loaded default Unilib conversion handle" has scrolled by, the SQL server is up and running.

9. As the sybase operating system user, run the following scripts:

```
isql  -Usa  -P<sa password>  -n  -i$SYBASE/scripts/installmaster
isql  -Usa  -P<sa password>  -n  -i$SYBASE/scripts/installcommit
isql  -Usa  -P<sa password>  -n  -i$SYBASE/scripts/instmsgs.ebf
```

10. Unmount the HP OpenView Performance Insight Sybase EBF CD-ROM, turn on trendtimer and make a backup of all databases.

You are finished.

Data Protector Hints and Tips

Problem with SAPDB backup on DP 5.5

PROBLEM: An upgrade was made to Data Protector 5.5. While file system backups are working fine, backups of a SAPDB directory are failing:

This test cell is made up of the following two hosts:

1. "mstrcntl", an rp5450 running HP-UX B.11.11. This server is our new DP 5.5 Cell Manager. It is known by its public interface card as "mstrcntl" and by its private interface card as "private_rp5450".

2. "tux.MYDOMAIN.local", an ML530/G2 running SLES8 Linux. This server is our new DP 5.5 SAP DB client. It is known by its public interface card as "tux" and by its private interface card as "private_ml530".

Both servers' network routing rules are configured such that all intra-server communications rely upon the private network. Both DP clients pass their "Check Installation" tests with 100% perfection.

PREVIEW BACKUP

The backup starts off OK, executing the initial dbmcli commands. However, as soon as it starts the media agent (which for purposes of this testing phase is a File Library on the CM), it immediately generates warning message 90:390:

```
[Warning] From: BMA@mstrcntl "DP_File_Library_mstrcntl_1"  Time: 1/19/2005 2:28:18 PM Cannot
delete the expired file depot "/DP_File_Library/c0000227541ee6a3753aa35001a.fd"
```

Nine seconds later, this message is generated:

```
[Normal] From: BMA@mstrcntl "DP_File_Library_mstrcntl_1"  Time: 1/19/2005 2:28:27 PM
ABORTED Media Agent "DP_File_Library_mstrcntl_1"
```

Chapter 3 (page 265) of the Integration Guide says to expect the file /var/opt/omni/tmp/<Backup_Specification_Name>_TEST_FILE after the test. No such file exists after the preview.

ACTUAL BACKUP

As with the preview backup, the initial dbmcli commands appear to be executed just fine. However, about one minute after the dbmcli command "backup_start", these messages are generated:

```
[Critical] From: OB2BAR_SAPDBBAR@tux "SMS"  Time: 1/19/2005 2:43:53 PM
       Error connecting BAR2 to DMA.

[Major] From: BSM@mstrcntl "private_ml530_SMS"  Time: 1/19/2005 2:43:53 PM
[61:1005]       Got unexpected close from OB2BAR Backup DA on private_ml530.

[Critical] From: OB2BAR_SAPDBBAR@tux "SMS"  Time: 01/19/05 14:44:55
       Error: SAPDB responded with:

   -24920,ERR_BACKUPOP: backup operation was unsuccessful
   The backup tool failed with 2 as sum of exit codes.

    The database request was canceled and ended with error -903.
```

At this point, the SAPDB diagnosis files were examined. It can be clearly seen the "-24920" error, which just says the "backup operation was unsuccessful". The External Backup Protocol log includes a reference to "-903" which suggests a "hostfile I/O error". Finally, in the Database Errors log, the "error occured, basis_err 3700". Nothing anywhere identifies what this last error means.

CONFIGURATION
Operating System - HP-UX
Version -
Product - data protector

RESOLUTION: Concerning the Preview backup issue:

The error "Cannot delete the expired file depot" error when performing the preview can be resolved by simply setting the data protection to 1 day to get around that issue.

Regarding the regular backup issue:

It turned out that the "dma" agent on tux wanted to send commands back to itself, but the /usr/omni/config/client/allow_hosts file was preventing it. Add the localhost address (127.0.0.1) to that file (actually added it to all allow_hosts files cell-wide just for good measure), and then the SAPDB backup was able to succeed.

The ’localhost/allow_hosts‘ issue was discovered from closely examining the files on "tux.hb.local” in /usr/omni/tmp

DP Disk Agent error when installing on Solaris 10: 'Unsupported architecture'

PROBLEM: Problem Definition:

The following error occurs when attempting to install a Disk Agent for DataProtector (DP) A.05.50 on a Solaris 10 system:

```
Status: zeno-b.iasl.ca.boeing.com : Aborted   : Unsupported
architecture                      : 0 %
[Critical]  zeno-b.iasl.ca.boeing.com: Unsupported architecture/OS
type
        (SunOS zeno 5.10 Generic_118844-26 i86pc i386 i86pc)
        Skipping client!
```

CONFIGURATION
Operating System - Sun Solaris
Version - A.05.50
Product - data protector

RESOLUTION:

The DataProtector Solaris agents are only certified to run on Sparc hardware and are not compatible with i386 hardware.

Data Protector - fails with 'Error message from likeywlib', 'could not load SSF library libsapsecu'

PROBLEM
When DataProtector attempts to backup SAP 7.0 with Oracle 10g, it fails with the following error messages as seen from a partial session report:

```
BR1301W Error message from likeywlib:
===...could not load SSF library libsapsecu.so
BR1301W Error message from likeywlib: likey_init: Couldn't load
SAPSECULIB ("libsapsecu.so") using function SsfSupInit (), rc = 10.
BR1302E Initialization of license key library likeywlib failed,
return code 1
BR0602E No valid SAP license found - please contact SAP
```

CONFIGURATION
Operating System - HP-UX
Application - Data Protector

RESOLUTION
The environment variable DIR_LIBRARY was needed to satisfy a requirement for SAP's brbackup so that brbackup could find the SAP library - libsapsecu.so. This variable was added to the environment with the following commands:

```
# cd /opt/omni/lbin

# ./util_cmd_putopts SAP <SID> DIR_LIBRARY '/usr/sap/<SID>/SYS/exe/run' \
-sublist Environment
```

Data Protector - error message during restore: Binary util_orarest.exe failed

PROBLEM
DataProtector restore produces the following message:

```
"[12:8346] Binary util_orarest failed. Cannot get
 information from remote host"
```

CONFIGURATION
Operating System - HP-UX
Subsystem - Data Protector 5.5, Oracle Integration

RESOLUTION
The error occurred because the util_orarest.exe was hung in the system call dlopen(3C). This hang was caused by the latest linker patch PHSS_35379.

This error was resolved by removing this patch. This issue is currently under investigation.

Data Protector - ZDB backup fails; Script 'obkbackup' failed to start

PROBLEM
After upgrading DataProtector to A.05.50, an oracle ZDB backup fails with the following message:

```
[Major] From: ob2rman.exe@...
    Script 'obkbackup' failed to start.
```

When the following message appears in the original session report, an additional backup session has been started, and it fails with:

```
[Warning] From: BSM@... ""  Time: 08/25/06 14:37:03
Bad characters in the group item name.

[Critical] From: BSM@... ""  Time: 8/25/2006 2:37:03 PM
None of the Disk Agents completed successfully.
Session has failed.

[Normal] From: BSM@... ""  Time: 8/25/2006 2:37:03 PM

  Backup Statistics:
        Session Queuing Time (hours)        0.00
        ---------------------------------------
        Completed Disk Agents ........      0
        Failed Disk Agents ...........      0
        Aborted Disk Agents ..........      0
```

The oracle8.log and the OB2BAR debugs contain the following:

```
    [Major] From: OB2BAR@... "name"  Time: 08/25/06 12:37:03
    Received ABORT request from BSM (ERR: Backup specification
    not found on Cell Manager. )
```

CONFIGURATION
Operating System - HP-UX
Version - 11.x
Application - DataProtector A.05.50

RESOLUTION
The issue described above is a known problem that occurs because the BARTYPE is not being passed to sbtinit. This causes another BSM session to be opened from application host for backup of the DP managed control file.

A special binary - QXCM1000361895pa.shar - has successfully resolved this behavior. HP engineers who encounter this issue are encouraged to open a new GR8 case with the EC OV SS team to request this binary.

DataProtector - OB2BAR agents die as soon as the start in Oracle integration

PROBLEM
In a DataProtector/Oracle integration, OB2BAR agents are dying and so a backup cannot be done. These OB2BAR agents apparently die just as they start. Attempts to backup to a local null device fail because of the OB2BAR 2 hour timeout. For example:

```
    [Normal] From: BMA@... "NULL device"  Time: 08/22/06 14:48:46
        STARTING Media Agent "NULL device"

    [Normal] From: BMA@... "NULL device"  Time: 08/22/06 14:48:47
        /dev/null
        Initializing new medium: "Default File_3"

    [Major] From: BSM@...  "CAT_whole_incr0"  Time: 08/22/06
    16:49:11 [61:1002]
        The OB2BAR Backup DA named "CAT" on host ...
        reached its inactivity timeout of 7200 seconds.
        The agent on host will be shutdown.
```

CONFIGURATION
Operating System - HP-UX
Version - 11.x
Subsystem - Data Protector 5.50

RESOLUTION
The OB2BAR agents were dying because the NLS_LANG is used by Oracle and was set to

"american_america.we8iso8859p1". This setting needed to be added to DataProtector OB2BAR's configuration that Oracle started. Here is the command needed to put this setting into the configuration file:

```
/opt/omni/lbin/util_cmd -putopt Oracle8 CAT NLS_LANG
american_america.we8iso8859p1 -sublist Environment
```

Once this was done, the backups started to work as expected.

DataProtector - error after adding check logical in gui; invalid RMAN backup script

PROBLEM
If the string "check logical" is added in the following location in the DataProtector GUI editor, then the following pop-up message occurs:

```
backup check logical incremental level <incr_level>
```

Here is the pop-up message from the GUI after the above is inserted:

```
[12:15913]  Cannot proceed, invalid RMAN backup script.
```

CONFIGURATION
Operating System - HP-UX
Version - 11.x
Subsystem - Data Protector / Oracle Integration

RESOLUTION
Even though Oracle accepts this as a valid rman command, the DataProtector GUI parser cannot accept it. The parser is highly dependent on position of the syntax. The following will work for DataProtector and also for Oracle:

```
backup incremental level <incr_level>
format 'dlb_oracle_10.1.0_tucker<WDB_%s:%t:%p>.dbf'
check logical
database;
```

DataProtector - tapes are marked as poor; I/O error message in debug log

PROBLEM
On an HP-UX 11i system in a SAN environment, Data Protector (DP) A.05.50 marks tapes as poor leaving fewer tapes available for backups. There are no related error messages in the session reports, but messages similar to the following are in the debugs:

```
12/01/06 20:58:09 BMA.1323.0["ma/dev/devseq.c /main/dp55/dp55_fix
/8":3266] A.05.50 bPHSS_34501/PHSS_34502/DPSOL_00209

SeqWrite: write() I/O error. Tape drive status:
SeqWrite:  SK  : 00h
    ASC : 00h
    ASCQ: 00h
```

```
....
SeqOp: (/dev/rmt/4mn):
ioctl(MTIOCTOP, mt_op=0, mt_count=1) fails: {13}
.....
SeqStat: **** Caught signal for SCSI BUS RESET!!! ****
```

It is unclear whether the DP media pool or the tape device is causing this behavior.

CONFIGURATION
Operating System - HP-UX
Version - 11.i
Application - DataProtector A.05.50

RESOLUTION
In a SAN environment it is essential to have DP locknames configured for the tape drives, and to ensure that other software and activities, are not accessing the DP tapes and drives. If these things are done correctly, errors like those above are unlikely to be seen.

In this particular case, the tapes were being incorrectly identified as poor due to an issue with the Fibre connection to the SAN. This behavior and the resulting errors, were not caused by DP.

DataProtector - error when restoring Oracle database; cannot connect to media agent,invalid hostname

ISSUE:

The following message occurs when attempting to restore an Oracle database using Data Protector (DP) A.05.10:

"Cannot connect to Media Agent on system [hostname.domain], port 53970 (IPC Invalid Hostname or IP Address System error: #UNKNOWN DNS ERROR#) => aborting."

SOLUTION:

This issue occurs when gethostbyname(3N) fails; it is not a Data Protector issue. This issue is resolved by installing the latest libc cumulative patch. As of the date of this writing, the latest libc patch is:

[PHCO_35743/PACHRDME/English]
Title: s700_800 11.11 libc cumulative patch

NOTE: Please apply this patch and any required dependencies. This patch, as with any patch, may be superseded. Please check for the latest patches at HP's IT Resource Center (ITRC) at the following web site: http://www.itrc.hp.com

Here is an excerpt from the debug file:

```
[112] [IpcGetHostByName] gethostbyname "hostname.domain"
[112] 2007-01-18 15:41:33 ("lib/ipc/ipc.c /main/dp51/r51_fix/
13":1529) A.05.10 bPHSS_34321/DPSOL_00190
[112] [IpcGetHostByName] gethostbyname returned 0000000000000000,
h_errno=0
[112] [IpcGetHostByName] Forcing retry. Reason: gethostbyname
```

```
returned NULL and h_errno = 0
[ 60] [IpcGetHostByName] h_errno=0 (~#UNKNOWN DNS ERROR#),
1200 retries left
```

DataProtector - Oracle backup hangs when cancelling mirror device

PROBLEM

During a DataProtector backup, when cancelling a mirror device, an Oracle backup will hang. There is no hanging problem when cancelling the primary device, just the mirror. Here is the barlist that was used:

```
BARLIST "IMIF_AR"
OWNER "ora920" "dba" "computer.company.domain"
GROUP "ARCHIVE_BACKUP"
DYNAMIC 1 1
POSTEXEC "/prod/backup/statdat_check.sh AT IMIF_AR  ORACLE8" -on_host
computer.company.domain

MIRROR 1
{
    DYNAMIC 1 1

    DEVICE "LTOMIL_1"
    {
         -sync
         -mp_preferred_host "computer.company.domain"
         -pool "ITAARCHLTO"
    }

    DEVICE "LTOMIL_3"
    {
         -sync
         -mp_preferred_host "computer.company.domain"
         -pool "ITAARCHLTO"
    }
}

DEVICE "MSLMIL_1"
{
     -sync
     -mp_preferred_host "computer.company.domain"
     -pool "ITAARCHMSL"
}

DEVICE "MSLMIL_3"
{
     -sync
     -mp_preferred_host "computer.company.domain"
     -pool "ITAARCHMSL"
}

CLIENT "IMIF" computer.company.domain
{
        -exec ob2rman.exe
        -args {
                "-backup"

        }
        -input {
                "run {"
                "allocate channel 'dev_1' type 'sbt_tape'"
                "parms 'ENV=(OB2BARTYPE=Oracle8,OB2APPNAME=IMIF,
OB2BARLIST=IMIF_AR)';"
                "backup filesperset 10"
                "format 'IMIF_AR<IMIF_%s:%t:%p:%c>.dbf'"
                "archivelog all delete input"
                ";"
                "}"
        }
        -profile
       -mirrorno 1
}  -protect weeks 2 -keepcatalog weeks 10
```

CONFIGURATION
Operating System - HP-UX
Subsystem - DataProtector Media Agent

RESOLUTION
The hanging behavior definitely occurred in the Backup Session Manager (BSM) and only when cancelling the mirror device. This was solved by a set of special binaries produced by the lab:

```
QXCM1000327531-6.txt
QXCM1000327531-6.shar
QXCM1000327531-6-IA.txt
QXCM1000327531-6-IA.shar
```

DataProtector - EVA/SMISA error, cannot connect to cell server, insufficient permissions

PROBLEM
An EVA/SMISA backup reports the following error:

```
[Major] From: SMISA@[...] "SMISA"  Time: 25/10/2006 15:28:33
[236:6000]      Cannot connect to the cell server.
     (Insufficient permissions. Access denied.)
```

Also, this is found in the debugs of the SMISA:

```
[ 99] 2006-10-25 15:28:33 ("cs/csa/mcsa.c /main/dp55/32":630)
A.05.50 bDPWIN_00194
[ 99] <<=== (4) }  /* MCsaGetAcl */
[ 99]
[ 54] [IRdbHandler::IRdbHandler()] *WARNING* Does not have the
minimal ACLs required: ACL_BACKUP|ACL_B_DATALIST|ACL_B_D_SAVE
[ 54] [IRdbHandler::IRdbHandler()] Destroying the
```

instance/connection.

[*The solution to this issue appears to be missing in the original EPing! Article – Ed.*]

DataProtector - cannot configure sybase instance after installing patch

PROBLEM
After installing the following patch on an HP-UX 11.23 PA-Risc server with DataProtector (DP) 5.5, it is impossible to properly configure a Sybase instance in DataProtector. The "util_sybase.exe -CONFIG" command works but the "util_sybase.exe -CHKCONF" always fails with RETVAL*8210*.

```
  [PHSS_34975/PACHRDME/English]
     s700_800 11.X OV DP5.50 PA RISC patch - SYBASE packet
```

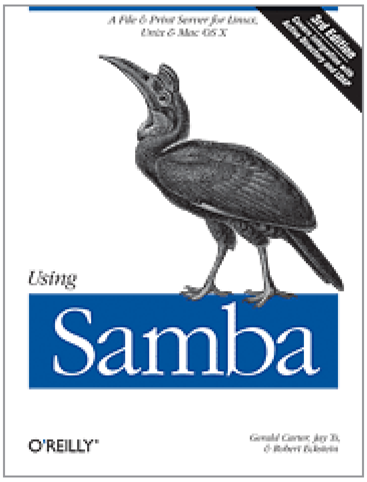
CONFIGURATION
Operating System - HP-UX
Version - 11.x
Subsystem - DataProtector 5.50

RESOLUTION
The issue is that the util_sybase.exe script did not take into account that the HP-UX 11.23 operating system was not an ia64 machine and was making bad decisions.

Book Reviews

"Using Samba" – Third Edition

By Gerald Carter, Jay Ts, Robert Eckstein
Third Edition January 2007
Pages: 447


A File & Print Server for Linux, Unix & Mac OS X
Using
Samba
O'REILLY
Gerald Carter, Jay Ts, & Robert Eckstein

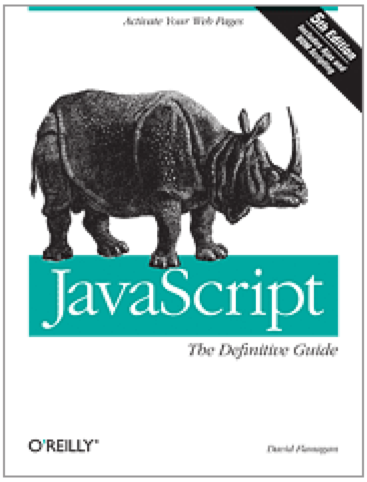
This book is the comprehensive guide to Samba administration, officially adopted by the Samba Team. Wondering how to integrate Samba's authentication with that of a Windows domain? How to get Samba to serve Microsoft Dfs shares? How to share files on Mac OS X?

These and a dozen other issues of interest to system administrators are covered. A whole chapter is dedicated to troubleshooting!

More Information - http://www.oreilly.com/catalog/samba3

"JavaScript: The Definitive Guide" – Fifth Edition

By David Flanagan
Fifth Edition August 2006
Pages: 1018



The indispensable reference for JavaScript programmers since 1996, *JavaScript: The Definitive Guide*, 5th Edition is completely revised and expanded to cover JavaScript as it is used in today's Web 2.0 applications.

More Information - JavaScript: The Definitive Guide, Fifth Edition

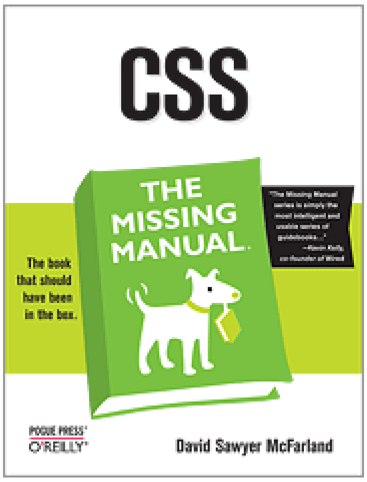
“CSS: The Missing Manual”

By David Sawyer McFarland First Edition August 2006
Pages: 494

Cascading Style Sheets are now a reliable method for handling all kinds of Web page presentations -- from fonts and colors to page layout. But due to CSS's complexity most designers treat it as a kind of window-dressing to spruce up the appearance of their sites without tapping into the real power of CSS.

CSS: The Missing Manual clearly explains this powerful design tool and how you can use it to build sparklingly new Web sites, or refurbish old sites that are ready for an upgrade.

More information - CSS: The Missing Manual



Cisco Security Vulnerabilities

Cisco IPv6 Routing Header Vulnerability

HP customers using Cisco networking kit should be aware of these....

From the Internet Storm Centre

Cisco vulnerabilities
Published: 2007-01-24,
Last Updated: 2007-01-24 22:23:04 UTC
by Maarten Van Horenbeeck (Version: 2)

IPv6 Routing Header vulnerability (cisco-sa-20070124-IOS-IPv6)

http://www.cisco.com/en/US/products/products_
security_advisory09186a00807cb0fd.shtml

Certain crafted IPv6 Type 0 routing headers could crash a device running IOS.

NOTES:

If you run Cisco switches or routers in your network, we advise you to review these bulletins in detail and take action where required. As a form of triage we believe organizations are most likely to be affected by the 'Crafted IP Option vulnerability', which also has the highest potential impact.

UPDATE:

Cisco has also released separate "Applied Intelligence Response" bulletins. These contain high quality information on how to detect exploitation of these vulnerabilities, and how they can be mitigated.

Most organizations will need to perform a code upgrade for at least some of these vulnerabilities - while testing the new releases, these documents may prove useful.

Cisco Crafted IP Option vulnerability

HP customers using Cisco networking kit should be aware of these....

From the Internet Storm Centre

Cisco vulnerabilities
Published: 2007-01-24,
Last Updated: 2007-01-24 22:23:04 UTC
by Maarten Van Horenbeeck (Version: 2)

Crafted IP Option vulnerability (cisco-sa-20070124-crafted-ip-option)

http://www.cisco.com/en/US/products/products_security_advisory09186a00807cb157.shtml

By sending certain ICMP, PIMv2, PGM or URD packets with a specific IP option set to a Cisco IOS or IOS XR device, an attacker could cause the device to reload or even execute arbitrary code. This applies to a wide variety of releases.

NOTES:

If you run Cisco switches or routers in your network, we advise you to review these bulletins in detail and take action where required. As a form of triage we believe organizations are most likely to be affected by the 'Crafted IP Option vulnerability', which also has the highest potential impact.

UPDATE:

Cisco has also released separate "Applied Intelligence Response" bulletins. These contain high quality information on how to detect exploitation of these vulnerabilities, and how they can be mitigated.

Most organizations will need to perform a code upgrade for at least some of these vulnerabilities - while testing the new releases, these documents may prove useful.

Cisco Crafted TCP Packet can cause denial of service

HP customers using Cisco networking kit should be aware of these....

From the Internet Storm Centre

Cisco vulnerabilities
Published: 2007-01-24,
Last Updated: 2007-01-24 22:23:04 UTC
by Maarten Van Horenbeeck (Version: 2)

Crafted TCP Packet can cause denial of service
(cisco-sa-20070124-crafted-tcp)

http://www.cisco.com/en/US/products/products_security_advisory09186a00807cb0e4.shtml

A remotely-exploitable memory leak in the Cisco IOS software could lead to a denial of service condition. This vulnerability applies to much of the IOS 12.0, 12.1 and 12.2 code base.

NOTES:

If you run Cisco switches or routers in your network, we advise you to review these bulletins in detail and take action where required. As a form of triage we believe organizations are most likely to be affected by the 'Crafted IP Option vulnerability', which also has the highest potential impact.

UPDATE:

Cisco has also released separate "Applied Intelligence Response" bulletins. These contain high quality information on how to detect exploitation of these vulnerabilities, and how they can be mitigated.

Most organizations will need to perform a code upgrade for at least some of these vulnerabilities - while testing the new releases, these documents may prove useful.

HP Security Bulletins – HP-UX

Document ID: c00717872
Version: 2
HPSBUX02129 SSRT061149 rev.2 - HP-UX running SLP, Remote Unauthorized Access

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-03-05

Last Updated: 2007-03-05

Potential Security Impact: Remote Unauthorized Access

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY

A potential security vulnerability has been identified in HP-UX when running Service Locator Protocol (SLP).The vulnerability could be exploited by a remote user of Service Locator Protocol (SLP) for unauthorized access.

References: SUSE-SA:2005:015

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed: HP-UX B.11.11, B.11.23

BACKGROUND

For a PGP signed version of this security bulletin please write to: security-alert@hp.com

SLP implementation on HP-UX is based on OpenSLP version 0.8.0 developed by Caldera Systems, Inc.

To determine if an HP-UX system has an affected version, search the output of "swlist -a revision -l fileset" for one of the filesets listed below. For affected systems verify that the recommended action has been taken.

AFFECTED VERSIONS

> HP-UX B.11.11
upgrade_SLP.INETSVCS-RUN
action: install revision 1.2 or subsequent
> URL: http://software.hp.com

HP-UX B.11.23
InternetSrvcs.INETSVCS2-RUN
action: install PHNE_33508 or subsequent

END AFFECTED VERSIONS

RESOLUTION

HP has made the following patch and web upgrade available to resolve this issue.

B.11.23 PHNE_33508 or subsequent

The patch can be retrieved from: http://itrc.hp.com

> The B.11.11 SLP Revision 1.2 update can be retrieved from:

http://software.hp.com

PRODUCT SPECIFIC INFORMATION

HP-UX Software Assistant: HP-UX Software Assistant is an enhanced application that replaces HP-UX Security Patch Check. It analyzes all HP-issued Security Bulletins and lists recommended actions that may apply to a specific HP-UX system. It can also download patches and create a depot automatically.

For more information see:

https://www.hp.com/go/swa

MANUAL ACTIONS: Yes - Update

HP-UX B.11.11 Update to HP-UXSLP Revision 1.2 or subsequent HP-UX B.11.23 No manual actions

HISTORY:

Version: 1 (rev.1) 25 September 2006 Initial release
Version: 2 (rev.2) 06 March 2007 Updated web upgrade location for B.11.11

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

SUPPORT COMMUNICATION - SECURITY BULLETIN
Document ID: c00771742
Version: 3
HPSBUX02153 SSRT061181 rev.3 - HP-UX Running Firefox, Remote Unauthorized Access or Elevation of Privileges or Denial of Service (DoS)

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2006-09-20

Last Updated: 2007-02-27

Potential Security Impact: Remote unauthorized access or elevation of privileges or Denial of Service (DoS)

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY

Potential security vulnerabilities have been identified in Firefox running on HP-UX. These vulnerabilities could be exploited remotely resulting in unauthorized access, elevation of privileges, or Denial of Service (DoS).

References:

> Mozilla Foundation Security Advisory (MFSA) 2006-73, 2006-72, 2006-71, 2006-70, 2006-69, 2006-68, 2006-67, 2006-66, 2006-65, 2006-64, 2006-62, 2006-61, 2006-60, 2006-59, 2006-58, 2006-57, 2006-56, 2006-55, 2006-54, 2006-53, 2006-52, 2006-51, 2006-50, 2006-48, 2006-47, 2006-46, 2006-45, 2006-44, 2006-43, 2006-42, 2006-41, 2006-39, 2006-38, 2006-37, 2006-36, 2006-35, 2006-34, 2006-33, 2006-32, 2006-31, 2006-30, 2006-29, 2006-28, 2006-27, 2006-25, 2006-24, 2006-23, 2006-22, 2006-20.

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.

> Firefox prior to version 1.5.0.9 running on HP-UX B.11.11 and B.11.23.

BACKGROUND

For a PGP signed version of this security bulletin please write to:
security-alert@hp.com

For further information please refer to:

http://www.mozilla.org/projects/security/known-vulnerabilities.html

AFFECTED VERSIONS

HP-UX B.11.11
HP-UX B.11.23
Firefox.FFOX-COM
> action: install preliminary version of Firefox 1.5.0.9 available from mozilla.org
> URL: ftp://ftp.mozilla.org/pub/mozilla.org/firefox/releases/1.5.0.9/contrib/

END AFFECTED VERSIONS

RESOLUTION

> Preliminary versions of Firefox 1.5.0.9 are available to resolve the potential vulnerabilities. These preliminary versions have received minimal testing and are localized for English only.

The preliminary versions are available for download from the following URL:

> ftp://ftp.mozilla.org/pub/mozilla.org/firefox/releases/1.5.0.9/contrib/

For HP-UX B.11.23 (IA):
> firefox_1.5.0.9_ia.depot.gz
> firefox_1.5.0.9_ia.depot.gz.readme

For HP-UX B.11.11 and B.11.23 (PA):
> firefox_1.5.0.9_pa.depot.gz
> firefox_1.5.0.9_pa.depot.gz.readme

> This security bulletin will be revised when fully tested and localized versions of Firefox 1.5.0.9 or subsequent for HP-UX are available.

> The most recent fully tested and localized Firefox (version 1.5.0.8) is available here:

http://www.hp.com/products1/unix/java/firefox/index.html

> Firefox version 1.5.0.8 does not resolve the following: Mozilla Foundation Security Advisory (MFSA) 2006-73, 2006-72, 2006-71, 2006-70, 2006-69, 2006-68. These are resolved in Firefox version 1.5.0.9.

MANUAL ACTION: Yes - Update
> install preliminary version of Firefox 1.5.0.9 available from mozilla.org

PRODUCT SPECIFIC INFORMATION

HP-UX Software Assistant: HP-UX Software Assistant is an enhanced application that replaces HP-UX Security Patch Check. It analyzes all HP-issued Security Bulletins and lists recommended actions that may apply to a specific HP-UX system. It can also download patches and create a depot automatically.

For more information see https://www.hp.com/go/swa

HISTORY

Version:1 (rev.1) - 20 September 2006 Initial release
Version:2 (rev.2) - 29 November 2006 preliminary Firefox 1.5.0.8 available
Version:3 (rev.3) - 27 February 2007 preliminary Firefox 1.5.0.9 available

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

SUPPORT COMMUNICATION - SECURITY BULLETIN
Document ID: c00863839
Version: 1
HPSBUX02192 SSRT061233 rev.1 - HP-UX Running ARPA Transport, Local Denial of Service (DoS)

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-02-12

Last Updated: 2007-02-12

Potential Security Impact: Local Denial of Service (DoS)

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY

A potential security vulnerability has been identified with HP-UX running ARPA transport. The vulnerability could be exploited by a local user to create a Denial of Service (DoS).

References: none

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed. HP-UX B.11.11 and B.11.23 running ARPA transport

BACKGROUND

For a PGP signed version of this security bulletin please write to:
security-alert@hp.com

AFFECTED VERSIONS

HP-UX B.11.11
Networking.NET-KRN
Networking.NET-RUN
Networking.NET2-KRN
Networking.NMS2-KRN
OS-Core.CORE2-KRN
action: install PHNE_35183 or subsequent

HP-UX B.11.23
Networking.NET-KRN
Networking.NET-RUN
Networking.NET2-KRN
Networking.NMS2-KRN
OS-Core.CORE2-KRN
action: install PHNE_35182 or subsequent

END AFFECTED VERSIONS

RESOLUTION

HP has provided the following patches to resolve this potential vulnerability.

These patches are available on http://itrc.hp.com

HP-UX B.11.11 - PHNE_35183 or subsequent
HP-UX B.11.23 - PHNE_35182 or subsequent

MANUAL ACTIONS: No

PRODUCT SPECIFIC INFORMATION

HP-UX Software Assistant: HP-UX Software Assistant is an enhanced application that replaces HP-UX Security Patch Check. It analyzes all HP-issued Security Bulletins and lists recommended actions that may apply to a specific HP-UX system. It can also download patches and create a depot automatically.

For more information see https://www.hp.com/go/swa

HISTORY

Version:1 (rev.1) 12 February 2007 Initial release

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

SUPPORT COMMUNICATION - SECURITY BULLETIN
Document ID: c00874667
Version: 1
HPSBUX02195 SSRT061237 rev.1 - HP-UX Running Software Distributor (SD), Remote Denial of Service (DoS)

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-02-27

Last Updated: 2007-02-27

Potential Security Impact: Remote Denial of Service (DoS)

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY

A potential security vulnerability has been identified with the version of GZIP delivered by HP-UX Software Distributor (SD). The vulnerability could be remotely exploited leading to a Denial of Service (DoS).

References: CVE-2006-4334, CVE-2006-4335, CVE-2006-4336, CVE-2006-4337, CVE-2006-4338

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP-UX B.11.11 and B.11.23 running Software Distributor (SD)

BACKGROUND

For a PGP signed version of this security bulletin please write to: security-alert@hp.com

To determine if an HP-UX system has an affected version, search the output of "swlist -a revision -l fileset" for one of the filesets listed below. For affected systems verify that the recommended action has been taken.

AFFECTED VERSIONS

HP-UX B.11.11

SW-DIST.GZIP
SW-DIST.SD-AGENT
SW-DIST.SD-CMDS
action: install PHCO_35587 or subsequent

HP-UX B.11.23
SW-DIST.GZIP
SW-DIST.SD-AGENT
SW-DIST.SD-CMDS
action: install revision B.11.23.0612 or subsequent
URL: http://docs.hp.com/en/SD

END AFFECTED VERSIONS

RESOLUTION

HP has made available the patch and the following upgrade package to resolve this issue.

HP-UX B.11.11 - PHCO_35587 or subsequent from: http://itrc.hp.com
HP-UX B.11.23 - SD update to B.11.23.0612 retrieved from: http://docs.hp.com/en/SD

MANUAL ACTIONS: Yes - Update
HP-UX B.11.11 - No manual actions
HP-UX B.11.23 - Update to HP-UX SD B.11.23.0612 or subsequent.

PRODUCT SPECIFIC INFORMATION

HP-UX Software Assistant: HP-UX Software Assistant is an enhanced application that replaces HP-UX Security Patch Check. It analyzes all HP-issued Security Bulletins and lists recommended actions that may apply to a specific HP-UX system. It can also download patches and create a depot automatically.

For more information see: https://www.hp.com/go/swa

HISTORY:

Version: 1 (rev.1) - 27 February 2007 Initial Release

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

SUPPORT COMMUNICATION - SECURITY BULLETIN
Document ID: c00805100
Version: 2
HPSBUX02174 SSRT061239 rev.2 HP-UX Running OpenSSL Denial of Service (DoS), Increase Privilege

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2006-11-08

Last Updated: 2006-12-18

Potential Security Impact: Remote Denial of Service (DoS)

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY

Potential security vulnerabilities have been identified with OpenSSL on HP-UX where the vulnerability could be exploited remotely to create a Denial of Service (DoS), or a local increase of priviledge.

References: CVE-2006-2937 CVE-2006-2940 CVE-2006-3738 CVE-2006-4343
CVE-2005-2969

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed. HP-UX B.11.11 and B.11.23

BACKGROUND

For a PGP signed version of this security bulletin please write to:
security-alert@hp.com

AFFECTED VERSIONS

HP-UX B.11.11
openssl.OPENSSL-CER
openssl.OPENSSL-CONF
openssl.OPENSSL-INC
openssl.OPENSSL-LIB
openssl.OPENSSL-MIS
openssl.OPENSSL-PRNG
openssl.OPENSSL-PVT
openssl.OPENSSL-RUN
> action: install revision A.00.09.07l or subsequent
URL: http://h20293.www2.hp.com/portal/swdepot/
displayProductInfo.do?productNumber=OPENSSL11I

HP-UX B.11.23
openssl.OPENSSL-CER
openssl.OPENSSL-CONF
openssl.OPENSSL-INC
openssl.OPENSSL-LIB
openssl.OPENSSL-MIS
openssl.OPENSSL-PRNG
openssl.OPENSSL-PVT
openssl.OPENSSL-RUN
> action: install revision A.00.09.07l.001 or subsequent
URL: http://h20293.www2.hp.com/portal/swdepot/
displayProductInfo.do?productNumber=OPENSSL11I

END AFFECTED VERSIONS

RESOLUTION

HP has made the following upgrade package available from

http://h20293.www2.hp.com/portal/swdepot/

displayProductInfo.do?productNumber=OPENSSL11I

MANUAL ACTIONS: Yes - Update

PRODUCT SPECIFIC INFORMATION

HP-UX Security Patch Check: Security Patch Check revision B.02.00 analyzes all HP-issued Security Bulletins to provide a subset of recommended actions that potentially affect a specific HP-UX system.

For more information:
http://software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=B6834AA
HISTORY:

Version 1 (rev.1) - 20 November 2006 Initial Release
Version 2 (rev.2) - 18 December 2006 Clarified applicable revision

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

SUPPORT COMMUNICATION - SECURITY BULLETIN
Document ID: c00815112
Version: 2
HPSBUX02178 SSRT061267 rev.2 - HP-UX Secure Shell Remote Unauthorized Denial of Service (DoS)

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2006-12-01

Last Updated: 2006-12-05

Potential Security Impact: Remote Denial of Service (DoS)

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY

A potential security vulnerability has been identified with HP-UX running HP-UX Secure Shell. The vulnerability could be remotely exploited to allow a remote unauthorized user to create a Denial of Service (DoS).

References: CVE-2006-0225, CVE-2006-4924

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed. >HP-UX B.11.11, B.11.23

BACKGROUND

For a PGP signed version of this security bulletin please write to:
security-alert@hp.com

To determine if an HP-UX system has an affected version, search the output of "swlist -a revision -l fileset" for one of the filesets listed below. For affected systems verify that the recommended action has been taken.

AFFECTED VERSIONS

HP-UX B.11.11
Secure_Shell.SECURE_SHELL
action: install revision A.04.40.006 or subsequent
URL: http://h20293.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=T1471AA

HP-UX B.11.23
Secure_Shell.SECURE_SHELL
action: install revision A.04.40.007 or subsequent
URL: http://h20293.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=T1471AA

END AFFECTED VERSIONS

RESOLUTION

HP is providing the following HP Secure Shell (T1471AA) updates to resolve this potential vulnerability.

These updates can be downloaded from

http://h20293.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=T1471AA

HP-UX B.11.11 - HP-UX Secure Shell A.04.40.006 HP-UX B.11.23 - HP-UX Secure Shell A.04.40.007

The HP-UX Secure Shell A.04.40.006 and A.04.40.007 are based on OpenSSH 4.4p1, and contain the following libraries: zlib1.2.3, OpenSSL v0.9.7l and TCP Wrappers v7.6-ipv6.4.

MANUAL ACTIONS: Yes - Update

Download and install the appropriate update from

http://h20293.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=T1471AA

PRODUCT SPECIFIC INFORMATION

HP-UX Security Patch Check: Security Patch Check revision B.02.00 analyzes all HP-issued Security Bulletins to provide a subset of recommended actions that potentially affect a specific HP-UX system.

For more information:
http://software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=B6834AA

HISTORY:

Version: 1 (rev.1) 04 December 2006 Initial release
Version: 2 (rev.2) 05 December 2006 Updated affected OS releases.

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

SUPPORT COMMUNICATION - SECURITY BULLETIN
Document ID: c00837319
Version: 2
HPSBUX02181 SSRT061289 rev.2 - HP-UX Running IPFilter, Remote Unauthorized Denial of Service (DoS)

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-01-16

Last Updated: 2007-02-05

Potential Security Impact: Remote unauthorized Denial of Service (DoS)

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY

A potential security vulnerability has been identified with HP-UX running IPFilter in combination with PHNE_34474. The vulnerability could be exploited by a remote unauthorized user to create a Denial of Service (DoS).

References: none

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed. HP-UX B.11.23 running IPFilter with PHNE_34474 installed.

BACKGROUND

For a PGP signed version of this security bulletin please write to:
security-alert@hp.com

A successful exploit will result in a system crash.

To determine if an HP-UX system has an affected version, search the output of "swlist -a revision -l fileset" for one of the filesets listed below. For affected systems verify that the recommended action has been taken.

AFFECTED VERSIONS

HP-UX B.11.23
IPF-HP.IPF-MIN
> action: remove the patch, disable IPFilter, or install preliminary patch

END AFFECTED VERSIONS

RESOLUTION

Until a patch is available to resolve the issue, the potential vulnerability can be avoided in three ways:

(1) remove PHNE_34474 on HP-UX B.11.23 systems where IPFilter is in use or

(2) disable IPFilter or

> (3) install the preliminary patch, UNOF_35938.depot, or manually install libnet.a.

To Determine Whether IPFilter is in Use:

If 'ipfstat -io' returns the following, then IPFilter is not in use:

```
# ipfstat -io

empty list for ipfilter(in)

empty list for ipfilter(out)
```

Alternative 1 - Remove PHNE_34474

If IPFilter is in use, PHNE_34474 can be removed to avoid the potential vulnerability.

Note that removing PHNE_34474 exposes the system to the possibility of a memory leak:

SR:8606414192 CR:JAGaf74051 - Connection oriented DLPI streams may see a small memory leak in rare conditions.

The patch documentation for PHNE_34474 should be consulted for a list of the other changes provided by PHNE_34474.

Alternative 2 - Disable IPFilter

Since IPFilter can be used as a defense against many types of exploits, the potential security impact should be considered before disabling IPFilter.

To disable IPFilter:

1. edit /etc/rc.config.d/ipfconf and set IPF_CONF and IPMON_START to 0.
2. run '/sbin/init.d/ipfboot stop'
3. run 'ipfstat -io' as discussed above to verify that IPFilter is no longer in use.

> Alternative 3 - Install UNOF_35938.depot or preliminary libnet.a

A preliminary patch is available. The library which resolves the vulnerability is also available for manual installation.

The instructions and the patch files are available from hprc.external.hp.com
(192.170.19.100):

ftp://ss061289:SS061289@hprc.external.hp.com/

The instructions are in: HPSBUX061289_README.txt
cksum: 3912651470 2828
md5sum: 5b2506b16fb97a1ac11ac8ed93eaa1fa

MANUAL ACTIONS: Yes - NonUpdate
HP-UX B.11.23 - Remove PHNE_34474 if installed or disable IPFilter or install preliminary patch

PRODUCT SPECIFIC INFORMATION

HP-UX Security Patch Check: Security Patch Check revision B.02.00 analyzes all HP-issued Security Bulletins to provide a subset of recommended actions that potentially affect a specific HP-UX system.

For more information:
http://software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=B6834AA

HISTORY

Version:1 (rev.1) 16 January 2007 Initial release
Version:2 (rev.2) 5 February 2007 UNOF_35938.depot available

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

SUPPORT COMMUNICATION - SECURITY BULLETIN
Document ID: c00849540
Version: 1
HPSBUX02186 SSRT071299 rev.1 - HP-UX running Apache Remote Execution of Arbitrary Code, Denial of Service (DoS), Unauthorized Access

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-01-17

Last Updated: 2007-01-23

Potential Security Impact: Remote execution of arbitrary code, Denial of Service (DoS), and unauthorized access.

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY

Potential security vulnerabilities have been identified with Apache running on HP-UX. These vulnerabilities could be exploited remotely to allow execution of arbitrary code, Denial of Service (DoS), or unauthorized access.

References: CVE-2006-2940, CVE-2006-2937, CVE-2006-3738, CVE-2006-4343, CVE-2006-4339, CVE-2005-2969.

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.
HP-UX B.11.11, B.11.23, and B.11.31 running Apache-based Web Server prior to v.2.0.58.01

BACKGROUND

For a PGP signed version of this security bulletin please write to:
security-alert@hp.com

AFFECTED VERSIONS

For IPv4:
HP-UX B.11.00
HP-UX B.11.11
hpuxwsAPACHE
action: install revision A.2.0.58.01 or subsequent restart Apache

URL: http://h20293.www2.hp.com/cgi-in/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=HPUXWSSUITE

For IPv6:
HP-UX B.11.11
hpuxwsAPACHE,revision=B.1.0.00.01
hpuxwsAPACHE,revision=B.1.0.07.01
hpuxwsAPACHE,revision=B.1.0.08.01
hpuxwsAPACHE,revision=B.1.0.09.01
hpuxwsAPACHE,revision=B.1.0.10.01
hpuxwsAPACHE,revision=B.2.0.48.00
hpuxwsAPACHE,revision=B.2.0.49.00
hpuxwsAPACHE,revision=B.2.0.50.00
hpuxwsAPACHE,revision=B.2.0.51.00
hpuxwsAPACHE,revision=B.2.0.52.00
hpuxwsAPACHE,revision=B.2.0.53.00
hpuxwsAPACHE,revision=B.2.0.54.00
hpuxwsAPACHE,revision=B.2.0.55.00
hpuxwsAPACHE,revision=B.2.0.56.00
hpuxwsAPACHE,revision=B.2.0.58.00
action: install revision B.2.0.58.01 or subsequent restart Apache
URL: http://h20293.www2.hp.com/cgi-in/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=HPUXWSSUITE

HP-UX B.11.23
hpuxwsAPACHE
action: install revision B.2.0.58.01 or subsequent restart Apache
URL: http://h20293.www2.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=HPUXWSSUITE

END AFFECTED VERSIONS

RESOLUTION

HP has made the following software updates available to resolve the issue. Software updates for the Apache-based Web Server are available from:
http://h20293.www2.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=HPUXWSSUITE

HP-UX B.11.00, B.11.11 and HP-UX B.11.23 require the Apache-based Web Server v.2.0.58.01 or subsequent.

Apache Update Procedure

Check for Apache Installation

To determine if the Apache web server from HP is installed on your system, use Software Distributor's swlist command. All three revisions of the product may co-exist on a single system.

For example, the results of the command swlist -l product | grep -I apache hpuxwsAPACHE B.2.0.55.00 HP-UX Apache-based Web Server

Stop Apache

Before updating, make sure the previous Apache binary is stopped. If Apache is not stopped, the installation would be successful but the new version would be prevented from starting until a later time.

After determining which Apache is installed, stop Apache with the following commands:
for hpuxwsAPACHE: /opt/hpws/apache[32]/bin/apachectl stop

Download and Install Apache

Download Apache from Software Depot.

http://h20293.www2.hp.com/cgi-bin/swdepot_parser.cgi/
cgi/displayProductInfo.pl?productNumber=HPUXWSSUITE

Verify successful download by comparing the cksum with the value specified on the installation web page.

Use SD to swinstall the depot. Installation of this new revision of HP Apache over an existing HP Apache installation is supported, while installation over a non-HP Apache is NOT supported.

Removing Apache Installation

The potential vulnerability can also be resolved by removing Apache rather than installing a newer revision. To remove Apache use both Software Distributor's "swremove" command and also "rm -rf" the home location as specified in the rc.config.d file "HOME" variables.
%ls /etc/rc.config.d | \ grep apache hpapache2conf hpws_apache[32]conf

MANUAL ACTIONS: Yes - Update plus other actions Install the revision of the product.

PRODUCT SPECIFIC INFORMATION

HP-UX Security Patch Check: Security Patch Check revision B.02.00 analyzes all HP-issued Security Bulletins to provide a subset of recommended actions that potentially affect a specific HP-UX system.

For more information:
http://software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=B6834AA

HISTORY: rev.1 - 23 January 2007 Initial Release

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

SUPPORT COMMUNICATION - SECURITY BULLETIN
Document ID: c00862809
Version: 1
HPSBUX02191 SSRT071302 rev.1 - HP-UX Running SLSd, Remote Unauthorized Arbitrary File Creation

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-02-12

Last Updated: 2007-02-12

Potential Security Impact: Remote unauthorized arbitrary file creation

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY

A potential security vulnerability has been identified with HP-UX running SLSd. The vulnerability could be exploited by a remote unauthorized user to create arbitrary files leading to root access.

References: none

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed. HP-UX B.11.11 running SLSd.

BACKGROUND

For a PGP signed version of this security bulletin please write to: security-alert@hp.com

The Hewlett-Packard Company thanks the iDefense Vulnerability Contributor Program for reporting this vulnerability to security-alert@hp.com.

AFFECTED VERSIONS

HP-UX B.11.11
criteria: if /etc/rc.config.d/slsd contains "SLSD_DAEMON=1"
Xserver.X11-SERV
action: run "/sbin/init.d/slsd stop", then set "SLSD_DAEMON=0" in /etc/rc.config.d/slsd.

END AFFECTED VERSIONS

RESOLUTION

To avoid the potential vulnerability disable SLSd as follows. SLDd should no longer be used. Disabling it will not affect functionality.

Run "/sbin/init.d/slsd stop".
Edit /etc/rc.config.d/slsd and set "SLSD_DAEMON=0"

MANUAL ACTIONS: Yes - NonUpdate
Run "/sbin/init.d/slsd stop", then set "SLSD_DAEMON=0" in /etc/rc.config.d/slsd.

PRODUCT SPECIFIC INFORMATION

HP-UX Software Assistant: HP-UX Software Assistant is an enhanced application that replaces HP-UX Security Patch Check. It analyzes all HP-issued Security Bulletins and lists recommended actions that may apply to a specific HP-UX system. It can also download patches and create a depot automatically.

For more information see https://www.hp.com/go/swa

HISTORY

Version:1 (rev.1) 12 February 2007 Initial release

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

SUPPORT COMMUNICATION - SECURITY BULLETIN
Document ID: c00876579
Version: 2
HPSBUX02196 SSRT071318 rev.2 - HP-UX Java (JRE and JDK) Remote Execution of Arbitrary Code

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-03-09

Last Updated: 2007-03-09

Potential Security Impact: Remote execution of arbitrary code.

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY

Java Runtime Environment (JRE) and Java Developer Kit (JDK) may allow a remote user to execute arbitrary code.

References: CVE-2007-0243, CVE-2006-6745, CVE-2006-6731

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.

HP-UX B.11.11 and B.11.23 running Java Runtime Environment (JRE) and Java Developer Kit (JDK):
Release 5.0.05 i.e., Release 1.5.0.05,
Release 1.4.2.11 and earlier,
Release 1.3.1.19 and earlier.

BACKGROUND

For a PGP signed version of this security bulletin please write to:
security-alert@hp.com

The Sun Java Runtime Environment (JRE) and Java Developer Kit (JDK) contain multiple vulnerabilities that can allow a remote, unauthenticated user to execute arbitrary code on a vulnerable system.

AFFECTED VERSIONS

NOTE: To determine if a system has an affected version, search the output of "swlist -a revision -l fileset" for an affected fileset. Then determine if a fixed revision or applicable patch is installed.

HP-UX B.11.11
HP-UX B.11.23
Jpi14.JPI14-COM
Jpi14.JPI14-COM-DOC
Jpi14.JPI14-IPF32
Jpi14.JPI14-PA11
Jdk14.JDK14-COM
Jdk14.JDK14-DEMO
Jdk14.JDK14-IPF32
Jdk14.JDK14-IPF64

Jdk14.JDK14-PA11
Jdk14.JDK14-PA20
Jdk14.JDK14-PA20W
Jdk14.JDK14-PNV2
Jdk14.JDK14-PWV2
Jre14.JRE14-COM
Jre14.JRE14-COM-DOC
Jre14.JRE14-IPF32
Jre14.JRE14-IPF32-HS
Jre14.JRE14-IPF64
Jre14.JRE14-IPF64-HS
Jre14.JRE14-PA11
Jre14.JRE14-PA11-HS
Jre14.JRE14-PA20
Jre14.JRE14-PA20-HS
Jre14.JRE14-PA20W
Jre14.JRE14-PA20W-HS
Jre14.JRE14-PNV2
Jre14.JRE14-PNV2-H
Jre14.JRE14-PWV2
Jre14.JRE14-PWV2-H
action:install revision 1.4.2.12.00 or subsequent.

Jdk15.JDK15-COM
Jdk15.JDK15-DEMO
Jdk15.JDK15-IPF32
Jdk15.JDK15-IPF64
Jdk15.JDK15-PA20
Jdk15.JDK15-PA20W
Jdk15.JDK15-PNV2
Jdk15.JDK15-PWV2
Jre15.JRE15-COM
Jre15.JRE15-COM-DOC
Jre15.JRE15-IPF32
Jre15.JRE15-IPF32-HS
Jre15.JRE15-IPF64
Jre15.JRE15-IPF64-HS
Jre15.JRE15-PA20
Jre15.JRE15-PA20-HS
Jre15.JRE15-PA20W
Jre15.JRE15-PA20W-HS
Jre15.JRE15-PNV2
Jre15.JRE15-PNV2-H
Jre15.JRE15-PWV2
Jre15.JRE15-PWV2-H
action:install revision 1.5.0.06 or subsequent

END AFFECTED VERSIONS

NOTE: The version number returned by "$java -version" and the version returned by swlist for Java are different. For example, when the $java -version is 5.0.6 the version shown by swlist is 1.5.0.06.

RESOLUTION

HP is providing the following Java updates to resolve the JRE potential vulnerability.

The updates are available from: http://www.hp.com/go/java

The HP website mentions Java 5.0, which can be recognized from the swlist -l fileset return value of 1.5.0.01.06.

These issues are addressed in the following versions of the HP Java:
* JDK and JRE 1.5.0.6 or subsequent,
* SDK and JRE 1.4.2.12 or subsequent,
* SDK and JRE 1.3.1.20 or subsequent.

If the latest version of Java is installed, older versions of Java may remain installed on the system. If these versions of Java are not needed, you may wish to remove them.

MANUAL ACTIONS: Yes - Update
For Java 1.5.0.00.00, update to Java 1.5.0.06 or subsequent.
> For Java 1.4.2.11 and earlier, update to revision 1.4.2.12 or subsequent.
For Java 1.3.1.19 or earlier, update to revision 1.3.1.20 so subsequent.

PRODUCT SPECIFIC INFORMATION

HP-UX Software Assistant: HP-UX Software Assistant is an enhanced application that replaces HP-UX Security Patch Check. It analyzes all HP-issued Security Bulletins and lists recommended actions that may apply to a specific HP-UX system. It can also download patches and create a depot automatically.

For more information see: https://www.hp.com/go/swa

HISTORY:

Version: 1 (rev.1) 06 March 2007 Initial release
Version: 2 (rev.2) 09 March 2007 Corrected typo in Manual Actions, in SSRT #.

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

SUPPORT COMMUNICATION - SECURITY BULLETIN
Document ID: c00854250
Version: 1
HPSBGN02187 SSRT061280 rev.1 - Mercury LoadRunner, Performance Center, Monitor over Firewall, Remote Unauthenticated Arbitrary Code Execution

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-02-07

Last Updated: 2007-02-07

Potential Security Impact: Remote unauthenticated arbitrary code execution

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY

A potential security vulnerability has been identified with the Mercury LoadRunner Agent, Performance Center Agent, and Monitor over Firewall. The vulnerability could be exploited by a remote unauthenticated user to execute arbitrary code.

References: ZDI-CAN-112

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed. Mercury LoadRunner Agent 8.1 SP1, FP1, FP2, FP3, and FP4 Mercury LoadRunner Agent 8.1 GA Mercury LoadRunner Agent 8.0 GA Mercury Performance Center Agent 8.1 FP1, FP2, FP3, and FP4 Mercury Performance Center Agent 8.1 GA Mercury Performance Center Agent 8.0 GA Mercury Monitor over Firewall 8.1 running on AIX, HP-UX, Linux, Solaris, and Windows NT.

BACKGROUND

For a PGP signed version of this security bulletin please write to:
security-alert@hp.com

For HP-UX:

AFFECTED VERSIONS

HP-UX B.11.11
action: if Mercury LoadRunner Agent, Performance Center Agent, or Monitor over Firewall is installed, apply the appropriate patch

END AFFECTED VERSIONS

RESOLUTION

HP has provided the following software patches to resolve this vulnerability.

Mercury LoadRunner Agent 8.1 FP4

LR81FP4P150 - SSRT061280 MA ZDI-CAN-112: Mercury LoadRunner Agent 8.1 FP4 Stack Overflow

http://webnotes.merc-int.com/patches.nsf/c4d68388a23535dc422567d0004bbae2/c337892f322b2311c22572670060b795?OpenDocument

LR81FP4P150(UNIX) - SSRT061280 MA ZDI-CAN-112: Mercury LoadRunner Agent 8.1 FP4 Stack Overflow

http://webnotes.merc-int.com/patches.nsf/c4d68388a23535dc422567d0004bbae2/6d7ce88c0d5c4b36c225726a004a94a2?OpenDocument

Mercury LoadRunner Agent 8.1 SP1, FP1, FP2, FP3

Upgrade to Mercury LoadRunner Agent 8.1 FP4 and apply the appropriate patch listed above.

Mercury LoadRunner Agent 8.1 GA

LR81P151 - SSRT061280 MA ZDI-CAN-112: Mercury LoadRunner Agent 8.1 Stack Overflow

http://webnotes.merc-int.com/patches.nsf/c4d68388a23535dc422567d0004bbae2/7cd789640e496c34c225726700613486?OpenDocument

LR81P151(UNIX) - SSRT061280 MA ZDI-CAN-112: Mercury LoadRunner Agent 8.1 Stack Overflow

http://webnotes.merc-int.com/patches.nsf/c4d68388a23535dc422567d0004bbae2/f2de896609dd7efbc225726a004af033?OpenDocument

Mercury LoadRunner Agent 8.0 GA

LR80P071 - SSRT061280 MA ZDI-CAN-112: Mercury LoadRunner Agent 8.0 Stack Overflow

http://webnotes.merc-int.com/patches.nsf/c4d68388a23535dc422567d0004bbae2/fa4a48afea2f8198c22572670061bbe7?OpenDocument

LR80P071(UNIX) - SSRT061280 MA ZDI-CAN-112: Mercury LoadRunner Agent 8.0 Stack Overflow

http://webnotes.merc-int.com/patches.nsf/c4d68388a23535dc422567d0004bbae2/5de153e30789fa4ac225726a004b2354?OpenDocument

Mercury Performance Center Agent 8.1 FP4

PC81FP4P155 - SSRT061280 MA ZDI-CAN-112: Mercury Performance Center Agent 8.1 FP4 Stack Overflow

http://webnotes.merc-int.com/patches.nsf/c4d68388a23535dc422567d0004bbae2/ae5d9a48a163fbb4c225726a004c7831?OpenDocument

PC81FP4P155(UNIX) - SSRT061280 MA ZDI-CAN-112: Mercury Performance Center Agent 8.1 FP4 Stack Overflow

http://webnotes.merc-int.com/patches.nsf/c4d68388a23535dc422567d0004bbae2/34e894d8d8a1b941c225726a004ff335?OpenDocument

Mercury Performance Center Agent 8.1 FP1, FP2, FP3

Upgrade to Mercury Performance Center Agent 8.1 FP4 and apply the appropriate patch listed above.

Mercury Performance Center Agent 8.1 GA

PC81P155 - SSRT061280 MA ZDI-CAN-112: Mercury Performance Center Agent 8.1 Stack Overflow

http://webnotes.merc-int.com/patches.nsf/c4d68388a23535dc422567d0004bbae2/0831f8b0bd9d9619c225726a004cf7fe?OpenDocument

PC81P155(UNIX) - SSRT061280 MA ZDI-CAN-112: Mercury Performance Center Agent 8.1 Stack Overflow

http://webnotes.merc-int.com/patches.nsf/c4d68388a23535dc422567d0004bbae2/a7333913152e65e1c225726a005035e4?OpenDocument

Mercury Performance Center Agent 8.0 GA

Upgrade to Mercury Performance Center Agent 8.1 GA and apply the appropriate patch listed above.

Mercury Monitor over Firewall 8.1

PC81P156 - SSRT061280 MA ZDI-CAN-112: Mercury Monitor over Firewall 8.1 Stack Overflow

http://webnotes.merc-int.com/patches.nsf/c4d68388a23535dc422567d0004bbae2/c9b9924b3206614fc225726a004ded7d?OpenDocument

Manual Actions: Yes - NonUpdate
If Mercury LoadRunner Agent, Performance Center Agent, or Monitor over Firewall is installed, apply the appropriate patch

PRODUCT SPECIFIC INFORMATION

HP-UX Security Patch Check: Security Patch Check revision B.02.00 analyzes all HP-issued Security Bulletins to provide a subset of recommended actions that potentially affect a specific HP-UX system.

For more information:
http://software.hp.com/portal/swdepot/
displayProductInfo.do?productNumber=B6834AA

HISTORY: Version: 1 (rev.1) 07 February 2007 Initial release

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

HP Security Bulletin – JetDirect

SUPPORT COMMUNICATION - SECURITY BULLETIN
Document ID: c00838612
Version: 1
HPSBPI02185 SSRT071290 rev.1 - HP Jetdirect Running ftp, Remote Denial of Service (DoS)

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-01-17

Last Updated: 2007-01-17

Potential Security Impact: Remote Denial of Service (DoS)

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY

A potential vulnerability has been identified with HP Jetdirect running ftp. The vulnerability could be exploited remotely to create a Denial of Service (DoS).

References: none

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed. HP Jetdirect running firmware versions from x.20.nn up to and including x.24.nn

BACKGROUND

For a PGP signed version of this security bulletin please write to:
security-alert@hp.com

The whitepaper 'HP Jetdirect Security Guidelines' has recommendations for securing HP Jetdirect.

The whitepaper is available here:
http://h20000.www2.hp.com/bc/docs/support/
SupportManual/c00746792/c00746792.pdf

RESOLUTION

This vulnerability can be resolved by upgrading the Jetdirect firmware. There is also a workaround for this vulnerability by making configuration changes.

Recent Jetdirect products use firmware revision x.25.nn or greater and are not vulnerable. Some older Jetdirect products allow the firmware to be upgraded and others do not.

Instructions for upgrading Jetdirect firmware are available here:
http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=bpj07429

For J4169A 610n - upgrade the firmware to version L.25.nn or greater.

For J6057A 615n - upgrade the firmware to version R.25.nn or greater.

Other older Jetdirect products running versions from x.20.nn up to and including x.24.nn are potentially vulnerable. The firmware for these products cannot be upgraded. The potential vulnerability can be avoided by disabling ftp or using access control lists as discussed in the whitepaper 'HP Jetdirect Security Guidelines' mentioned above.

PRODUCT SPECIFIC INFORMATION

HISTORY

Version:1 (rev.1) - 17 January 2007 Initial release

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

HP Security Bulletin – Microsoft Storage Management Appliance

SUPPORT COMMUNICATION - SECURITY BULLETIN
Document ID: c00846931
Version: 1
HPSBST02184 SSRT071296 rev.1 - Storage Management Appliance (SMA), Microsoft Patch Applicability MS07-001 Through MS07-004

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-01-16

Last Updated: 2007-01-16

Potential Security Impact: Please check the table below

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY

Various potential security vulnerabilities have been identified in Microsoft software that is running on the Storage Management Appliance (SMA). Some of these vulnerabilities may be pertinent to the SMA, please check the table in the Resolution section of this Security Bulletin.

References: MS07-001, MS07-002, MS07-003, MS07-004

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed. Storage Management Appliance v2.1 Software running on:

Storage Management Appliance I
Storage Management Appliance II
Storage Management Appliance III

BACKGROUND

For a PGP signed version of this security bulletin please write to:
security-alert@hp.com

Patches released by Microsoft after MS06-051 are covered by monthly Security Bulletins

For the full archived list of Microsoft security updates applicable for Storage Management Appliance software v2.1, please refer to the following Security Bulletins available on the IT Resource Center (ITRC) Web site:

http://www.itrc.hp.com/service/cki/secBullArchive.do

For patches released by Microsoft in 2003, MS03-001 to MS03-051 refer to Security Bulletin HPSBST02146
For patches released by Microsoft in 2004, MS04-001 to MS04-045 refer to Security Bulletin HPSBST02147
For patches released by Microsoft in 2005, MS05-001 to MS05-055 refer to Security Bulletin HPSBST02148
For patches released by Microsoft in 2006, MS06-001 to MS06-051 refer to Security Bulletin HPSBST02140

The Microsoft patch index archive and further details about all Microsoft patches can be found on the following Web site:

http://www.microsoft.com/technet/security/bulletin/summary.mspx

NOTE: The SMA must have all pertinent SMA Service Packs applied

Windows 2000 Update Rollup 1

Customers are advised to download and install the Windows 2000 Update Rollup 1 for Service Pack 4 on SMA v2.1. For more information please refer to the Windows 2000 Update Rollup 1 for Service Pack 4 and Storage Management Appliance v2.1 advisory at the following website:

http://h18004.www1.hp.com/products/sanworks/softwaredrivers/managementappliance/index.html

Windows 2000 Update Rollup 1 for SP4 does not include security updates released after April 30, 2005 starting from MS05-026. It also does not include patches MS04-003 and MS04-028. Please install these patches in addition to Windows 2000 Update Rollup 1 for SP4, if they have not been installed already

RESOLUTION

HP strongly recommends the immediate installation of all security patches that apply to third party software which is integrated with SMA software products supplied by HP, and that patches are applied in accordance with an appropriate patch management policy.

NOTE: Patch installation instructions are shown at the end of this table.

MS Patch
Analysis
Action

MS07-001 Vulnerability in Microsoft Office 2003 Brazilian Portuguese Grammar Checker Could Allow Remote Code Execution (921585) SMA does not have this component.

Patch will not run successfully.
Customers should not be concerned with this issue

MS07-002 Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (927198) SMA does not have this component.

Patch will not run successfully.
Customers should not be concerned with this issue

MS07-003 Vulnerabilities in Microsoft Outlook Could Allow Remote Code Execution (925938) SMA does not have this component.

Patch will not run successfully.
Customers should not be concerned with this issue

MS07-004 Vulnerability in Vector Markup Language Could Allow Remote Code Execution (929969) Possible security issue exists.

Patch will run successfully.
For SMA v2.1, customers should download patch from Microsoft and install.

Impacts only: Internet Explorer 6 SP1 - Or - Internet Explorer 5.01 SP4

To determine your IE version check the IE help page.

Installation Instructions: (if applicable)

Download patches to a system other than the SMA

Copy the patch to a floppy diskette or to a CD

Execute the patch by using Terminal Services to the SMA or by attaching a keyboard, monitor and mouse to the SMA.

The Microsoft Windows Installer 3.1 is supported on SMA v2.1. For more information please refer at the following website:

http://www.microsoft.com/downloads/details.aspx?FamilyID
=889482fc-5f56-4a38-b838-de776fd4138c&hash=SYSSXDF&displaylang=en

PRODUCT SPECIFIC INFORMATION

HISTORY Version: 1 (rev.1) - 16 January 2007 Initial release

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

SUPPORT COMMUNICATION - SECURITY BULLETIN
Document ID: c00870027
Version: 1
HPSBST02194 SSRT071306 rev.1 - Storage Management Appliance (SMA), Microsoft Patch Applicability MS07-005 Through MS07-016

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-02-21

Last Updated: 2007-02-21

Potential Security Impact: Please check the table below

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY

Various potential security vulnerabilities have been identified in Microsoft software that is running on the Storage Management Appliance (SMA). Some of these vulnerabilities may be pertinent to the SMA, please check the table in the Resolution section of this Security Bulletin.

References: MS07-005, MS07-006, MS07-007, MS07-008, MS07-009, MS07-010, MS07-011, MS07-012, MS07-013, MS07-014, MS07-015, MS07-016

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed. Storage Management Appliance v2.1 Software running on:

Storage Management Appliance I
Storage Management Appliance II
Storage Management Appliance III

BACKGROUND

For a PGP signed version of this security bulletin please write to:
security-alert@hp.com

Patches released by Microsoft after MS06-051 are covered by monthly Security Bulletins

For the full archived list of Microsoft security updates applicable for Storage Management Appliance software v2.1, please refer to the following Security Bulletins available on the IT Resource Center (ITRC) Web site:

http://www.itrc.hp.com/service/cki/secBullArchive.do

For patches released by Microsoft in 2003, MS03-001 to MS03-051 refer to Security Bulletin HPSBST02146
For patches released by Microsoft in 2004, MS04-001 to MS04-045 refer to Security Bulletin HPSBST02147

For patches released by Microsoft in 2005, MS05-001 to MS05-055 refer to Security Bulletin HPSBST02148
For patches released by Microsoft in 2006, MS06-001 to MS06-051 refer to Security Bulletin HPSBST02140

The Microsoft patch index archive and further details about all Microsoft patches can be found on the following Web site:

http://www.microsoft.com/technet/security/bulletin/summary.mspx

NOTE: The SMA must have all pertinent SMA Service Packs applied

Windows 2000 Update Rollup 1

Customers are advised to download and install the Windows 2000 Update Rollup 1 for Service Pack 4 on SMA v2.1. For more information please refer to the Windows 2000 Update Rollup 1 for Service Pack 4 and Storage Management Appliance v2.1 advisory at the following website:

http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=179111&taskId=101&prodTypeId=12169&prodSeriesId=315667

Windows 2000 Update Rollup 1 for SP4 does not include security updates released after April 30, 2005 starting from MS05-026. It also does not include patches MS04-003 and MS04-028. Please install these patches in addition to Windows 2000 Update Rollup 1 for SP4, if they have not been installed already

RESOLUTION

HP strongly recommends the immediate installation of all security patches that apply to third party software which is integrated with SMA software products supplied by HP, and that patches are applied in accordance with an appropriate patch management policy.

NOTE: Patch installation instructions are shown at the end of this table.

MS Patch
Analysis
Action

MS07-005 Vulnerability in Step-by-Step Interactive Training Could Allow Remote Code Execution (923723) Possible security issue exists.

Patch will run successfully.
For SMA v2.1, customers should download patch from Microsoft and install.

MS07-006 Vulnerability in Windows Shell Could Allow Elevation of Privilege (928255) SMA does not have this component.

Patch will not run successfully.
Customers should not be concerned with this issue

MS07-007 Vulnerability in Windows Image Acquisition Service Could Allow Elevation of Privilege (927802) SMA does not have this component.

Patch will not run successfully.
Customers should not be concerned with this issue

MS07-008 Vulnerability in HTML Help ActiveX Control Could Allow Remote Code Execution (928843) Possible security issue exists.

Patch will run successfully.
For SMA v2.1, customers should download patch from Microsoft and install.

MS07-009 Vulnerability in Microsoft Data Access Components Could Allow Remote Code Execution (927779) Possible security issue exists.

Patch will run successfully.
For SMA v2.1, customers should download patch from Microsoft and install.

MS07-010 Vulnerability in Microsoft Malware Protection Engine Could Allow Remote Code Execution (932135) SMA does not have this component.

Patch will not run successfully.
Customers should not be concerned with this issue

MS07-011 Vulnerability in Microsoft OLE Dialog Could Allow Remote Code Execution (926436) Possible security issue exists.

Patch will run successfully.
For SMA v2.1, customers should download patch from Microsoft and install.

MS07-012 Vulnerability in Microsoft MFC Could Allow Remote Code Execution (924667) Possible security issue exists.

Patch will run successfully.
For SMA v2.1, customers should download patch from Microsoft and install.

MS07-013

Vulnerability in Microsoft RichEdit Could Allow Remote Code Execution
(918118)
Possible security issue exists.

Patch will run successfully.
For SMA v2.1, customers should download patch from Microsoft and install.

MS07-014 Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (929434) SMA does not have this component.

Patch will not run successfully.
Customers should not be concerned with this issue

MS07-015

Vulnerabilities in Microsoft Office Could Allow Remote Code Execution
(932554)
SMA does not have this component.

Patch will not run successfully.
Customers should not be concerned with this issue

MS07-016 Cumulative Security Update for Internet Explorer (928090) Possible security issue exists.

Patch will run successfully.
For SMA v2.1, customers should download patch from Microsoft and install.

Impacts only: Internet Explorer 6 SP1 - or - Internet Explorer 5.01 SP4

To determine your IE version check the IE help page.

Installation Instructions: (if applicable)

Download patches to a system other than the SMA

Copy the patch to a floppy diskette or to a CD

Execute the patch by using Terminal Services to the SMA or by attaching a keyboard, monitor and mouse to the SMA.

The Microsoft Windows Installer 3.1 is supported on SMA v2.1. For more information please refer at the following website:

http://www.microsoft.com/downloads/details.aspx?FamilyID=889482fc-5f56-4a38-b838-de776fd4138c&hash=SYSSXDF&displaylang=en

HISTORY

Version: 1 (rev.1) - 20 February 2007 Initial release

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

HP Security Bulletin – HP OpenView

SUPPORT COMMUNICATION - SECURITY BULLETIN
Document ID: c00809525
Version: 1
HPSBMA02176 SSRT051035 rev.1 - HP OpenView Network Node Manager (OV NNM) Remote Unauthorized Execution of Arbitrary Code

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-01-10

Last Updated: 2007-01-10

Potential Security Impact: Remote unauthorized execution of arbitrary code

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY

A potential vulnerability has been identified with HP OpenView Network Node Manager (OV NNM). This vulnerability could be exploited remotely by an unauthorized user to execute arbitrary code with the permissions of the NNM server.

References: None

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed. HP OpenView Network Node Manager (OV NNM) 6.20, 6.4x, 7.01, 7.50 running on HP-UX B.11.00, B.11.11, and B.11.23, Solaris, Windows NT, Windows 2000, Windows XP, and Linux.

BACKGROUND

For a PGP signed version of this security bulletin please write to:
security-alert@hp.com

The Hewlett-Packard Company thanks Tenable Network Security for reporting this vulnerability to security-alert@hp.com.

To determine if a system has an affected version, search the output of "swlist -a revision -l fileset" for one of the filesets listed below. For affected systems verify that the recommended action has been taken.

AFFECTED VERSIONS

For HP-UX OV NNM 7.50
HP-UX B.11.23 (IA)
OVNNMgr.OVNNM-RUN
action: install PHSS_34099 or subsequent

HP-UX B.11.23 (PA)
HP-UX B.11.11
HP-UX B.11.00
OVNNMgr.OVNNM-RUN
action: install PHSS_34098 or subsequent

For HP-UX OV NNM 7.01
HP-UX B.11.00
HP-UX B.11.11
OVNNMgr.OVNNM-RUN
action: install PHSS_35579 or subsequent

For HP-UX OV NNM 6.4x
HP-UX B.11.00
HP-UX B.11.11
OVNNMgr.OVNNM-RUN
action: install PHSS_34202 or subsequent

For HP-UX OV NNM 6.20
HP-UX B.11.00
HP-UX B.11.11
OVNNMgr.OVNNM-RUN
action: install PHSS_35113 or subsequent

For Solaris OV NNM 7.50
SunOS 5.6
SunOS 5.7
SunOS 5.8
SunOS 5.9

action: install PSOV_03436 or subsequent

For Solaris OV NNM 7.01
SunOS 5.6
SunOS 5.7
SunOS 5.8
SunOS 5.9
action: install PSOV_03468 or subsequent

For Solaris OV NNM 6.4x
SunOS 5.6
SunOS 5.7
SunOS 5.8
SunOS 5.9
action: install PSOV_03437 or subsequent

For Solaris OV NNM 6.20
SunOS 5.6
SunOS 5.7
SunOS 5.8
SunOS 5.9
action: install PSOV_03461 or subsequent

For Windows OV NNM 7.50
Windows NT
Windows 2000
Windows XP
action: install NNM_01115 or subsequent

For Windows OV NNM 7.01
Windows NT
Windows 2000
Windows XP
action: install NNM_01147 or subsequent

For Windows OV NNM 6.4x
Windows NT
Windows 2000
Windows XP
action: install NNM_01116 or subsequent

For Windows OV NNM 6.20
Windows NT
Windows 2000
Windows XP
action: install NNM_01139 or subsequent

For Linux OV NNM 7.50
Linux RedHatAS2.1
action: install LXOV_00026 or subsequent

END AFFECTED VERSIONS

RESOLUTION
HP has provided the following patches to resolve this potential vulnerability. These patches are available from http://support.openview.hp.com/patches/

OpenView Network Node Manager 7.50

HP-UX B.11.23 (IA)
PHSS_34099 or subsequent

HP-UX B.11.23 (PA)
PHSS_34098 or subsequent

HP-UX B.11.11
PHSS_34098 or subsequent

HP-UX B.11.00
PHSS_34098 or subsequent

Linux RedHatAS2.1
LXOV_00026 or subsequent

Solaris
PSOV_03436 or subsequent

Windows
NNM_01115 or subsequent

OpenView Network Node Manager 7.01

HP-UX B.11.11
PHSS_35579 or subsequent

HP-UX B.11.00
PHSS_35579 or subsequent

Solaris
PSOV_03468 or subsequent

Windows
NNM_01147 or subsequent

OpenView Network Node Manager 6.4x

HP-UX B.11.11
PHSS_34202 or subsequent

HP-UX B.11.00
PHSS_34202 or subsequent

Solaris
PSOV_03437 or subsequent

Windows
NNM_01116 or subsequent

OpenView Network Node Manager 6.20

HP-UX B.11.11
PHSS_35113 or subsequent

HP-UX B.11.00
PHSS_35113 or subsequent

Solaris
PSOV_03461 or subsequent

Windows
NNM_01139 or subsequent

MANUAL ACTIONS: Non-HP-UX only. Install the patches listed in the Resolution section for Solaris, Windows NT, Windows 2000, Windows XP, and Linux.

PRODUCT SPECIFIC INFORMATION

HP-UX Security Patch Check: Security Patch Check revision B.02.00 analyzes all HP-issued Security Bulletins to provide a subset of recommended actions that potentially affect a specific HP-UX system.

For more information:
http://software.hp.com/portal/swdepot/displayProductInfo.do?productNumber=B6834AA

HISTORY Version:1 (rev.1) - 10 January 2007 Initial release

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

SUPPORT COMMUNICATION - SECURITY BULLETIN
Document ID: c00809410
Version: 1
HPSBMA02175 SSRT061174 rev.1 - HP OpenView Network Node Manager (OV NNM) Remote Unauthorized Read Access to Files

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-01-10

Last Updated: 2007-01-10

Potential Security Impact: Remote unauthorized read access to files

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY

A potential vulnerability has been identified with HP OpenView Network Node Manager (OV NNM). This vulnerability could be exploited remotely by an unauthorized user to gain read access to files with the permissions of the NNM server.

References: None

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed. HP OpenView Network

Node Manager (OV NNM) 6.20, 6.4x, 7.01, 7.50 running on HP-UX B.11.00, B.11.11, and B.11.23, Solaris, Windows NT, Windows 2000, Windows XP, and Linux.

BACKGROUND

For a PGP signed version of this security bulletin please write to:
security-alert@hp.com

To determine if a system has an affected version, search the output of "swlist -a revision -l fileset" for one of the filesets listed below. For affected systems verify that the recommended action has been taken.

AFFECTED VERSIONS

For HP-UX OV NNM 7.50
HP-UX B.11.23 (IA)
OVNNMgr.OVNNM-RUN
action: install PHSS_34871 or subsequent

HP-UX B.11.23 (PA)
HP-UX B.11.11
HP-UX B.11.00
OVNNMgr.OVNNM-RUN
action: install PHSS_34870 or subsequent

For HP-UX OV NNM 7.01
HP-UX B.11.00
HP-UX B.11.11
OVNNMgr.OVNNM-RUN
action: install PHSS_35579 or subsequent

For HP-UX OV NNM 6.4x
HP-UX B.11.00
HP-UX B.11.11
OVNNMgr.OVNNM-RUN
action: install PHSS_34949 or subsequent

For HP-UX OV NNM 6.20
HP-UX B.11.00
HP-UX B.11.11
OVNNMgr.OVNNM-RUN
action: install PHSS_35113 or subsequent

For Solaris OV NNM 7.50
SunOS 5.6
SunOS 5.7
SunOS 5.8
SunOS 5.9
action: install PSOV_03459 or subsequent

For Solaris OV NNM 7.01
SunOS 5.6
SunOS 5.7
SunOS 5.8
SunOS 5.9
action: install PSOV_03468 or subsequent

For Solaris OV NNM 6.4x
SunOS 5.6
SunOS 5.7
SunOS 5.8
SunOS 5.9
action: install PSOV_03460 or subsequent

For Solaris OV NNM 6.20
SunOS 5.6
SunOS 5.7
SunOS 5.8
SunOS 5.9
action: install PSOV_03461 or subsequent

For Windows OV NNM 7.50
Windows NT
Windows 2000
Windows XP
action: install NNM_01137 or subsequent

For Windows OV NNM 7.01
Windows NT
Windows 2000
Windows XP
action: install NNM_01147 or subsequent

For Windows OV NNM 6.4x
Windows NT
Windows 2000
Windows XP
action: install NNM_01138 or subsequent

For Windows OV NNM 6.20
Windows NT
Windows 2000
Windows XP
action: install NNM_01139 or subsequent

For Linux OV NNM 7.50
Linux RedHatAS2.1
action: install LXOV_00043 or subsequent

END AFFECTED VERSIONS

RESOLUTION

HP has provided the following patches to resolve this potential vulnerability. These patches are available from http://support.openview.hp.com/patches/

OpenView Network Node Manager 7.50

HP-UX B.11.23 (IA)
PHSS_34871 or subsequent

HP-UX B.11.23 (PA)

PHSS_34870 or subsequent

HP-UX B.11.11
PHSS_34870 or subsequent

HP-UX B.11.00
PHSS_34870 or subsequent

Linux RedHatAS2.1
LXOV_00043 or subsequent

Solaris
PSOV_03459 or subsequent

Windows
NNM_01137 or subsequent

OpenView Network Node Manager 7.01

HP-UX B.11.11
PHSS_35579 or subsequent

HP-UX B.11.00
PHSS_35579 or subsequent

Solaris
PSOV_03468 or subsequent

Windows
NNM_01147 or subsequent

OpenView Network Node Manager 6.4x

HP-UX B.11.11
PHSS_34949 or subsequent

HP-UX B.11.00
PHSS_34949 or subsequent

Solaris
PSOV_03460 or subsequent

Windows
NNM_01138 or subsequent

OpenView Network Node Manager 6.20

HP-UX B.11.11
PHSS_35113 or subsequent

HP-UX B.11.00
PHSS_35113 or subsequent

Solaris
PSOV_03461 or subsequent

Windows
NNM_01139 or subsequent

MANUAL ACTIONS: Non-HP-UX only. Install the patches listed in the Resolution section for Solaris, Windows NT, Windows 2000, Windows XP, and Linux.

PRODUCT SPECIFIC INFORMATION

HP-UX Security Patch Check: Security Patch Check revision B.02.00 analyzes all HP-issued Security Bulletins to provide a subset of recommended actions that potentially affect a specific HP-UX system.

For more information:
http://software.hp.com/portal/swdepot/
displayProductInfo.do?productNumber=B6834AA

HISTORY

Version:1 (rev.1) - 10 January 2007 Initial release

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

SUPPORT COMMUNICATION - SECURITY BULLETIN
Document ID: c00727143
Version: 3
HPSBMA02133 SSRT061201 rev.3 - HP Oracle for OpenView (OfO) Critical Patch Update

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2006-07-19

Last Updated: 2007-01-22

Potential Security Impact: Local or remote compromise of confidentiality, availability, integrity.

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY

Oracle(r)) has issued a Critical Patch Update which contains solutions for a number of potential security vulnerabilities. These vulnerabilities may be exploited locally or remotely to compromise the confidentiality, availability or integrity of Oracle for OpenView (OfO).

References: Oracle Critical Patch Update - January 2007

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed. Oracle for OpenView (OfO) versions 8.1.7, 9.1.01, and 9.2 running on HP-UX, Tru64 UNIX, Linux, Solaris, and Windows.

BACKGROUND

For a PGP signed version of this security bulletin please write to:
security-alert@hp.com

Oracle has issued Critical Patch Update - January 2007.

For more information:
http://www.oracle.com/technology/deploy/security/
critical-patch-updates/cpujan2007.html

Information about previous Oracle Critical Patch Updates can be found here:

http://www.oracle.com/technology/deploy/security/alerts.htm

The following products are affected:

Product Number
Description

ORA200BC
OfO v8.1.7 for HP-UX LTU

ORA200CA
OfO v9.2 64bit HP-UX 11&11.11 LTU

ORA205BC
OfO v8.1.7 for HP-UX 5 LTU Bundle

ORA205CA
OfO v9.2 64bit HP-UX 11&11.11 5 LTUs

ORA230BC
OfO v8.1.7 for HP-UX Media

ORA230CA
OfO v9.2 64bit HP-UX 11&11.11 Media Kit

ORA240BC
OfO v8.1.7 for HP-UX Eval LTU & Media

ORA300BC
OfO v8.1.7 for Win 2000/NT LTU

ORA300CA
OfO v9.2 32bit Windows LTU

ORA305BC
OfO v8.1.7 for Win 2000/NT 5 LTU Bundle

ORA305CA
OfO v9.2 32bit Windows 5 LTUs

ORA330BC
OfO v8.1.7 for Win 2000/NT Media

ORA330CA
OfO v9.2 32bit Windows Media Kit

ORA340BC

OfO v8.1.7 for Win 2000/NT Eval LTU

ORA400BC
OfO v8.1.7 for Sun Solaris LTU

ORA400CA
OfO v9.2 32bit Sun Solaris 2.7&2.8 LTU

ORA401CA
OfO v9.2 64bit Sun Solaris 2.7&2.8 LTU

ORA405BC
OfO v8.1.7 for Sun Solaris 5 LTU Bundle

ORA405CA
OfO v9.2 32bit Sun Solaris 2.7&2.8 5 LTU

ORA406CA
OfO v9.2 64bit Sun Solaris 2.7&2.8 5 LTU

ORA430BC
OfO v8.1.7 for Sun Solaris Media

ORA430CA
OfO v9.2 32bit Sun Solaris 2.7&2.8 Media

ORA431CA
OfO v9.2 64bit Sun Solaris 2.7&2.8 Media

ORA440BC
OfO v8.1.7 for Sun Solaris Eval LTU

ORA500CA
OfO v9.1.01 64bit Tru64 V5.1a LTU Ent.Ed

ORA505CA
OfO v9.1.01 64bit Tru64 V5.1a LTU

ORA530CA
OfO v9.1.01 64bit Tru64 V5.1a Media Kit

ORA600CA
OfO for Linux LTU

ORA605CA
OfO for Linux LTU Service Bureaus Bundle

ORA630CA
OfO v9.2.0 for Linux, Media Kit

AFFECTED VERSIONS

HP-UX B.11.11
HP-UX B.11.23
action: If Oracle for OpenView (OfO) is installed, install the Oracle Critical Patch Update - January 2007

END AFFECTED VERSIONS

Note: Since Oracle for OpenView (OfO) is not installed using swinstall(1M) the Security Patch Check Tool cannot determine whether it is present on an HP-UX system. Customer maintained configuration documentation should be consulted to determine whether Oracle for OpenView (OfO) is installed.

RESOLUTION

Oracle for OpenView (OfO) customers who have support contracts directly with Oracle should obtain the "Critical Patch Update - January 2007"from Oracle.

Oracle for OpenView (OfO) customers who have support with Hewlett-Packard should contact their normal support channel to obtain the "Critical Patch Update - January 2007."

For support contract information, please visit:

http://www.hp.com/managementsoftware/contract_maint

MANUAL ACTIONS : Yes - Update
Install the Oracle Critical Patch Update - January 2007.

Oracle is a registered U.S. trademark of the Oracle Corporation, Redwood City, California.

PRODUCT SPECIFIC INFORMATION

HP-UX Security Patch Check: Security Patch Check revision B.02.00 analyzes all HP-issued Security Bulletins to provide a subset of recommended actions that potentially affect a specific HP-UX system.

For more information:
http://software.hp.com/portal/swdepot/display
ProductInfo.do?productNumber=B6834AA

HISTORY

Version 1 (rev.1) - 19 July 2006 Initial release "Critical Patch Update - July 2006"
Version 2 (rev.2) - 23 October 2006 "Critical Patch Update - October 2006" is available
Version 3 (rev.3) - 22 January 2007 "Critical Patch Update - January 2007" is available

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

SUPPORT COMMUNICATION - SECURITY BULLETIN
Document ID: c00862204
Version: 1
HPSBMA02190 SSRT071300 rev.1 - HP OpenView Storage Data Protector, Local Execution of Arbitrary Code

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-02-07

Last Updated: 2007-02-07

Potential Security Impact: Local execution of arbitrary code

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY

A potential security vulnerability has been identified with HP OpenView Storage Data Protector running on HP-UX with PHSS_35149 or PHSS_35150 installed and Solaris with DPSOL_00229 installed. The vulnerability could be exploited by a local user to execute arbitrary code.

References: none

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed. HP OpenView Storage Data Protector 5.50 running on HP-UX B.11.00, B.11.11, or B.11.23 with PHSS_35149 or PHSS_35150 installed or running on Solaris with DPSOL_00229 installed.

BACKGROUND

For a PGP signed version of this security bulletin please write to:
security-alert@hp.com

For HP-UX

AFFECTED VERSIONS

HP-UX B.11.23 (IA)
DATA-PROTECTOR.OMNI-HPUX-P
action: install PHSS_35165 or subsequent

HP-UX B.11.23 (PA)
HP-UX B.11.11
HP-UX B.11.00
DATA-PROTECTOR.OMNI-HPUX-P
action: install PHSS_35164 or subsequent

END AFFECTED VERSIONS

RESOLUTION

HP has provided the following patches to resolve this potential vulnerability. These patches are available on http://itrc.hp.com

HP-UX B.11.23 (IA) - PHSS_35165 or subsequent

HP-UX B.11.23 (PA) - PHSS_35164 or subsequent

HP-UX B.11.11 - PHSS_35164 or subsequent

HP-UX B.11.00 - PHSS_35164 or subsequent

Solaris - DPSOL_00233 or subsequent

MANUAL ACTIONS: No

PRODUCT SPECIFIC INFORMATION

HP-UX Security Patch Check: Security Patch Check revision B.02.00 analyzes all HP-issued Security Bulletins to provide a subset of recommended actions that potentially affect a specific HP-UX system.

For more information:
http://software.hp.com/portal/swdepot/display
ProductInfo.do?productNumber=B6834AA

HISTORY: Version:1 (rev.1) 7 February 2007 Initial release

Third Party Security Patches: Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.

HP Security Bulletin – HP ServiceGuard

SUPPORT COMMUNICATION - SECURITY BULLETIN
Document ID: c00860750
Version: 1
HBSBGN02189 SSRT071297 rev.1 ServiceGuard for Linux, Remote Unauthorized Access

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2007-02-12

Last Updated: 2007-02-12

Potential Security Impact: Remote unauthorized access

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY

A potential security vulnerability has been identified with HP Serviceguard for Linux that may allow remote unauthorized access.

References: none

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.

HP Serviceguard for Linux:
SuSE SLES8 United Linux 1.0, prior to release SG A.11.15.07
SuSE SLES9 SLES10, prior to release SG A.11.16.10
RedHat Enterprise Linux, prior to release SG A.11.16.10

BACKGROUND

For a PGP signed version of this security bulletin please write to:
security-alert@hp.com

RESOLUTION

HP has made the following patches to resolve this potential security vulnerability.
These patches are available on http://itrc.hp.com
Retrieve applicable patches and install using applicable Linux tools.

SuSE SLES8 United Linux 1.0, release SG A.11.15.07

SLES8/UL1.0 IA32 SGLX_00070
SLES8/UL1.0 IA64 SGLX_00071

SuSE SLES9 SLES10, release SG A.11.16.10

SLES9 IA32 SGLX_00114
SLES9 IA64 SGLX_00115
SLES9 x86_64 SGLX_00116

SLES10 IA32 SGLX_00117
SLES10 IA64 SGLX_00118
SLES10 x86_64 SGLX_00119

RedHat Enterprise Linux, release SG A.11.16.10

RedHat3.0AS RedHat3.0ES IA32 SGLX_00099 RedHat3.0AS RedHat3.0ES IA64 SGLX_00100
RedHat3.0AS RedHat3.0ES x86_64 SGLX_00101

RedHat4AS RedHat4ES IA32 SGLX_00111
RedHat4AS RedHat4ES IA64 SGLX_00112
RedHat4AS RedHat4ES x86_64 SGLX_00113

PRODUCT SPECIFIC INFORMATION

HISTORY: Version:1 (rev.1) 12 February 2007 Initial release

Third Party Security Patches:
Third party security patches which are to be installed on systems running HP software products should be applied in accordance with the customer's patch management policy.