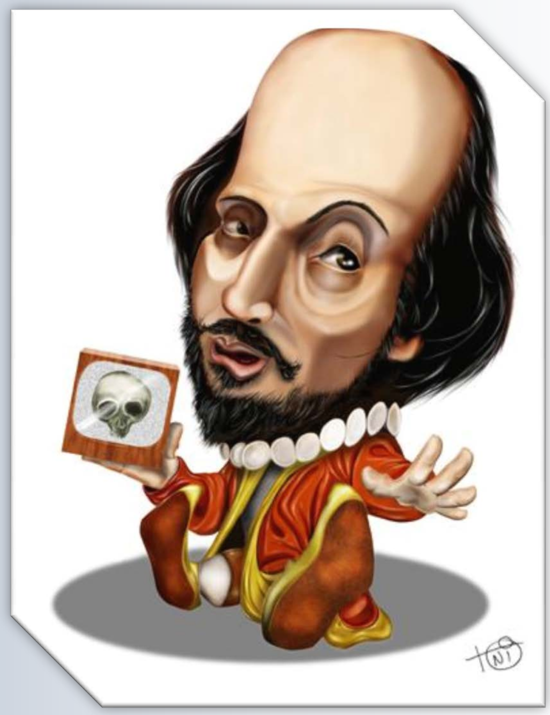
COMP 175
System Administration and Security



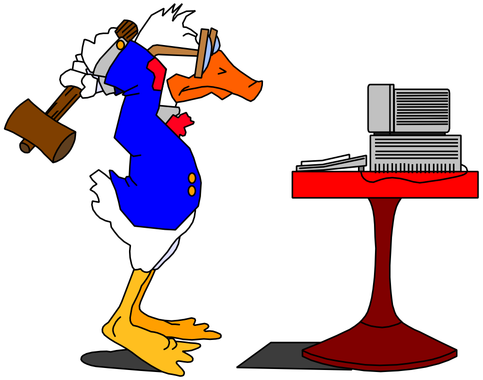
Backing Up Data

Yea, from the table of my memory,
I'll wipe away all trivial fond records.

-Hamlet Act I, scene 5, line 91

Data

- Information stored on computers is worth more than the computers themselves
  - Consider what you put on them
- Hundreds of ways to lose data
  - Accidental file deletion
  - External/Internal failures
- Backup - The most efficient and convenient way to protect your data
- Backup must be done carefully and on a regular schedule
- Consider yourself as the customer for now….



Backup Devices and Media

- Medium
- Capacity
- Cost
- Cost/GB
- Reusable
- Random (tape – no)
- Speed
- Lifespan - Most media use magnetic particles to store their data, these media are subject to damage by electrical and magnetic fields.

Logical backup

- Why?
  - Job security
  - Loss of data than can't be replaced
- Offsite storage
- Conventional vs. personal
- USB
- External drive
- Cloud
- Compression
- Virtualization – *where did the SAN go?*
  - *Whoops*

Physical backups

- Bit level backup
- Used for device level backup
- Used for OS recovery, recovery media
- Used for boot device recovery
- Used for disk device information
- Plenty of 3rd party products use for OS level recovery with “bootable backup” in addition to user data backup
- Forensic data recovery

Scope of Backup

- User data
- Business data
- Operating systems
- Configuration data (routers, systems, etc.)
- Physical and Virtualized
- Devices to ensure recovery

AHAJOKES.COM
MY COMPUTER DOESN'T WORK! THE HARD DRIVE CRASHED! WHAT DO I DO?!
DID YOU BACK UP?
WHY? IS IT GONNA BLOW?!
STEINFELD ©96

Backup Commands

- *A quick romp through the backup utilities—*
  - cp (duh)
  - ftp (eh)
  - rcp (no, no, no)
  - scp
  - rsync
  - tar
  - cpio
  - pax (see cpio, tar)
  - dump/restore – the standard

The usual suspects

- cp –rp source destination
- ftp hostname
  user
  name
  cd source or destination
  lcd destination/source
  put/get filename
  quit
- scp source user@destination:/pathtofile
  scp user@source:/pathtofile /destination
- rcp source user@destination:/pathtofile
  rcp user@ source:/pathtofile /destination
  uses .rhosts   -   see manpage on hosts.equiv

rsync

- rsync.samba.org   (for support)
- rsync copies files either to or from a remote host, or locally on the current host but not copying files between two remote hosts
- Reduces data sent over network - sends only differences between source files and existing files at destination
- Two different ways for rsync to contact a remote system:
  - Using a remote-shell program as the transport (such as ssh or rsh)
  - Contacting rsync daemon directly via TCP (man rsyncd.conf)
  - rsync –avh /source /destination
  - rsync -avze ssh /home/user/directory/ user@remotehost:home/user/directory/
- Other Options

  -a, --archive archive mode; equals

  -r, --recursive recurse into directories

  -u, --update - skip files that are newer on the receiver

Tape ARchive

- Oldest and most portable backup utility between systems
- Destination is always larger than source
- Use with compress
- Built-in compress (GNU command) is less portable
- Subject to errors, especially in extract (see cpio)
- `tar -cvf /archivefile /source1 /source2`
  - creates archive – Caution on relative versus absolute path archives
- `tar -tvf /archivefile`
  - List archive before extracting - Caution about extracts as root
- `tar -xvf  /archivefile`
  - Extract archive
- Other optiions:
  - -A append
  - -u update (refresh)
  - -z compress (GNU)

cpio

- Another UNIX backup utility – less portable than tar
- Can process native cpio or tar archives
  - Be careful with archive type.
- Uses STDIN/STDOUT for processing
  - Accepts filenames as input from STDIN
  - Archive is redirected STDOUT
  - Used with find to backup

Basic options:

-i --extract, extracts files from STDIN.
-o –create, reads STDIN, obtains list of path/names, copies files to STDOUT
-p --pass-through, reads STDIN, obtains list of path/names of files to STDOUT
-A –append, to archive
-c read or write header information in ASCII form for portability.
-v verbose
-d –make-directory
-t –list, archive contents
-H –format use specifies archive format
-F –file=archivename

cpio

```
find . -print | cpio -ocv > /dev/rmt0
```

Find command lists all files/directories piped to cpio & copy to tape

```
find . -print | cpio -dumpv /home/users/hope
```

Find all files/directories for cpio to copy to hope user account

```
cpio -icuvd < /dev/rmt0
```

Restore the files back from tape to the current directory

```
find -depth –print /export/home | cpio --create > /dev/rmt0
```

Creates an archive of the /export/home directory tree on tape

```
cpio --extract < /dev/rmt0
```

Restores all files from the archive in /dev/fd0 (since no files specified)

```
find /export/home –depth –print|cpio --create --file=/vol/ar0
```

Create archive to a specific file

```
cpio --list < /dev/rmt0
```

Lists all files in the archive.

pax – Portable Archive eXtract

- New front end for tar, cpio.   Developed under BSD.
- Processes both type of archives – tar, cpio
- Combines features of both commands
- Uses STDIN/STDOUT as default file source dest
- Options
  - -w write archive
  - -r read archive
  - -a append to archive
  - -v list archive
  - - f archive
  - -u refesh archive (ignore older than)
  - -x format types

pax examples

-
  ```
  pax -w -f /dev/rmt0 .
  ```
  Write current directory to tape

-
  ```
  pax -v -f filename
  ```
  View archive contents (to STDOUT)

-
  ```
  pax -w . >/dir/archive
  ```
  Write current directory to archive

-
  ```
  pax -r * </dir/archive
  ```
  Restore archive to current directory

-
  ```
  find c:/ -mtime 7 | pax -w >a:/archive
  ```
  Archive files modified in last 7 days (differential backup)

dump / restore

Original filesystem backup mechanism, most common LINUX utility

dump –options /dev/dumpdevice /source

Common dump options:

0-9 : 0=full, 1-9 incremental dump level

f : output file (tape), d : tape density

u update /etc/dumpdates file

Restore –options /dev/dumpdevice /destination

Common restore options:

i Interactive restoration of specified files

r restore filesystem

t List filenames on the backup archive

T extract to this directory

C Compare the contents of the archive with the current filesystem

x Only the named files are extracted from the archive

f Specify the archive file

v verbose output

```
dump -0f /dev.rmt0 /home          - Full  dump of home to tape
restore -rf /dev.rmt0 –T /home   - And a restore
```

dd

- Bit level backup. Uses STDIN/STDOUT like other utilities
- Misused, stands for Destoyed Data

Caution!! dd - copies until told to stop or end of input/output device

- Syntax:

dd if=inputdevorfile of=outputdevorfile bs=blocksize count=#blocks

- Basic options:

bs=BYTES

cbs=BYTES, see ibs, obs

conv=KEYWORDS – ascii,ibm,block,unblock,lcase,ucase,sync,noerror

count=BLOCKS

if=FILE

of=FILE

seek/skip #BLOCKS of output / input

dd examples

- dd if=/dev/zero /dev/sda

  Write binary zeros to disk. Destroy a disk
- dd if=dev/sda of=/dev/sdb conv=noerror,sync

  Clone a disk. Target must be exact C/H/S replica.
- dd if=dev/sda of=/mnt/someremovablemedia/sda.img

  Backup a disk
- dd if=/dev/hda2 of=/tmp/hda2.img

  Backup a partition
- dd if=/dev/sda of=/tmp/linux.mbr bs=512 count=1

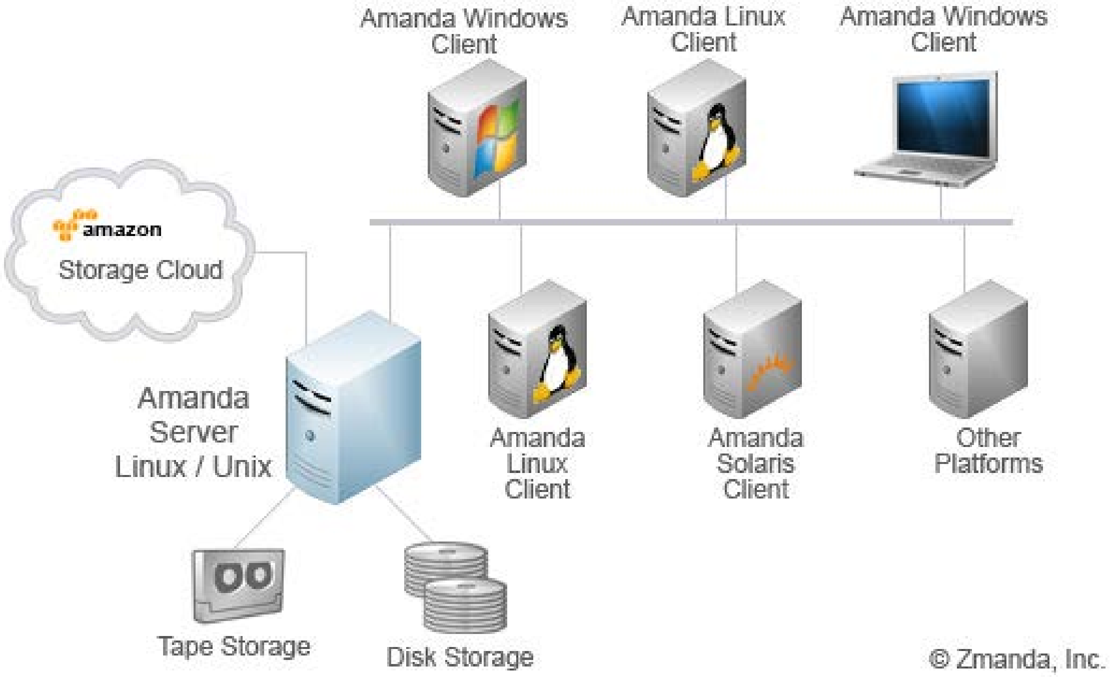
  Backup a MBR
- dd if=/dev/urandom of=f.doc bs=7166 count=1; rm f.doc

  Securely destroy file by writing random bits & removing it
- dd if=/dev/sdc1 count=1 skip=1000

  Examine block #1001 on sdc1

Backup Management

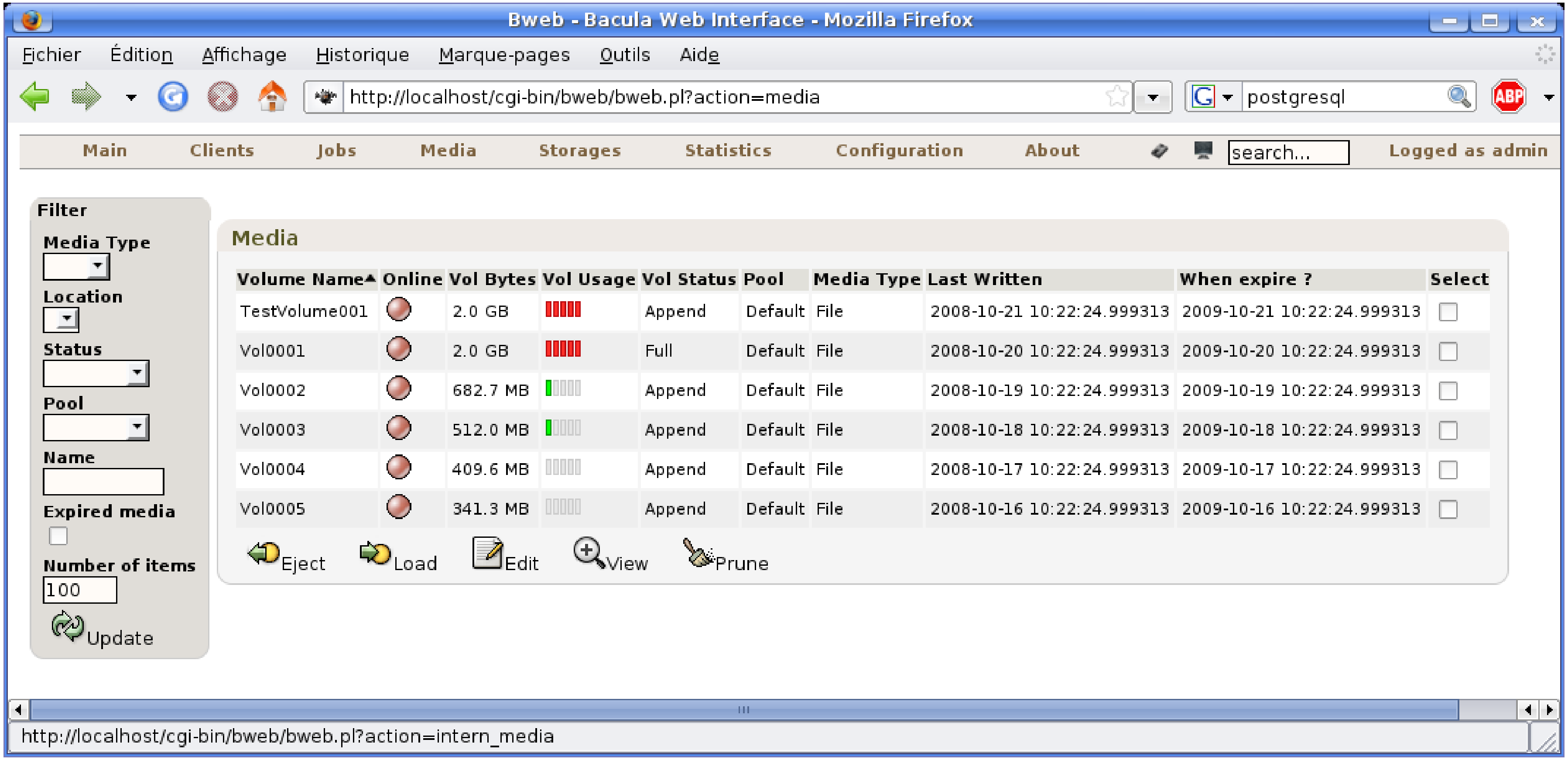
- Amanda (Open Source) Most popular tool
- Simplifies the CLI management
- Uses native dump and/or GNU tar
  - Community supported version
  - Enterprise (paid support)
  - Appliance



© Zmanda, Inc.

Backup Management

- Bacula (Open Source) (web interface shown)



Filter

Media Type

Location

Status

Pool

Name

Expired media □

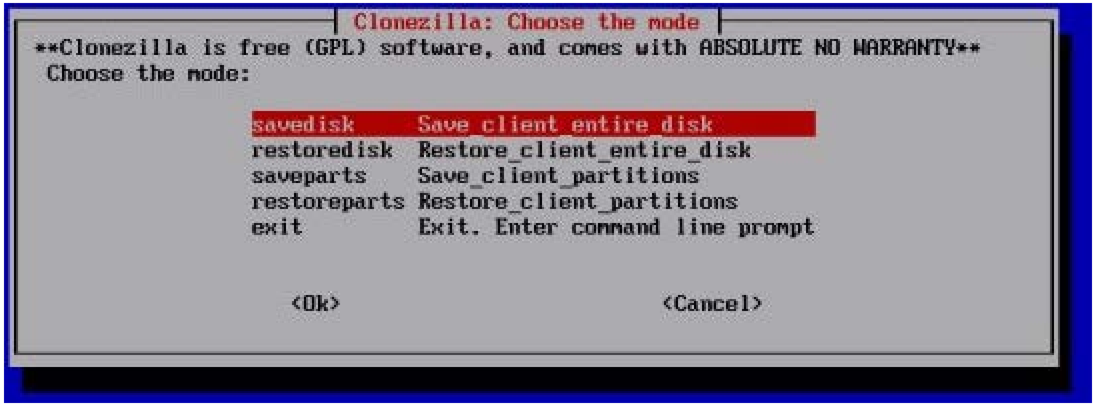
Number of items 100

Media

Volume Name▴	Online	Vol Bytes	Vol Usage	Vol Status	Pool	Media Type	Last Written	When expire ?	Select
TestVolume001	●	2.0 GB	🟥🟥🟥🟥🟥	Append	Default	File	2008-10-21 10:22:24.999313	2009-10-21 10:22:24.999313	□
Vol0001	●	2.0 GB	🟥🟥🟥🟥🟥	Full	Default	File	2008-10-20 10:22:24.999313	2009-10-20 10:22:24.999313	□
Vol0002	●	682.7 MB	🟩▯▯▯▯	Append	Default	File	2008-10-19 10:22:24.999313	2009-10-19 10:22:24.999313	□
Vol0003	●	512.0 MB	🟩▯▯▯▯	Append	Default	File	2008-10-18 10:22:24.999313	2009-10-18 10:22:24.999313	□
Vol0004	●	409.6 MB	▯▯▯▯▯	Append	Default	File	2008-10-17 10:22:24.999313	2009-10-17 10:22:24.999313	□
Vol0005	●	341.3 MB	▯▯▯▯▯	Append	Default	File	2008-10-16 10:22:24.999313	2009-10-16 10:22:24.999313	□

Backup Management

- Clonezilla (Open source clone of Ghost)

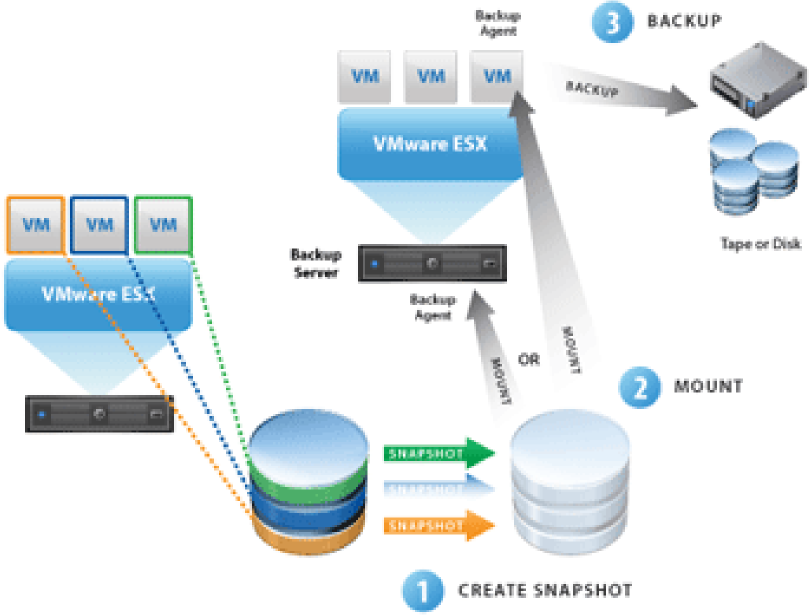


```
                   Clonezilla: Choose the mode
**Clonezilla is free (GPL) software, and comes with ABSOLUTE NO WARRANTY**
 Choose the mode:

                  savedisk      Save client entire disk
                  restoredisk   Restore_client_entire_disk
                  saveparts     Save_client_partitions
                  restoreparts  Restore_client_partitions
                  exit          Exit. Enter command line prompt


                     <Ok>                        <Cancel>
```

- VMware Consolidated Backup (Commercial)



Remote Backup Service

- Cloud as a backup service
- Sounds good, less costly, no staff needed
  - Fools believe things related to apps, data, identity security are magically solved by cloud
- Moves compressed data across Internet circuit
  - Most expensive and constrained circuit
  - "On average, a complete data restore takes a few days at most."
- "No per megabyte fees" "Predictable costs"
- SMB Offer $229yr – multiple servers – 250GB
- In 2009, admitted loss of backups of over 7,500 customers – blamed Promise Tech controllers

Backup In Context

- Backups are routine task
  - Test that they work
  - Worst case is a failure while backing up
- Backups also part of disaster recovery plan – strategic

- Large data losses often the result of lost backups
- A 2011 study of small businesses:
  - 81% consider data to be their most valuable asset
  - 57% lack a disaster recovery plan for data
  - 40-60% never re-open after a disaster (FEMA)
  - System/hardware failure accounts for 68% of data loss
  - Human error accounts for 32% of data loss

Designing a Backup Strategy

- Backup plan
- Written document that outlines:
  - When and how files are backed up
  - How files are stored
  - How files are restored

- Backup plan questions
  - What files should be backed up?
  - Who will back up files?
  - Where are files located?
  - How should backups be performed?
  - Must you be able to restore data within a specific period of time? (SLA)

Designing a Backup Strategy

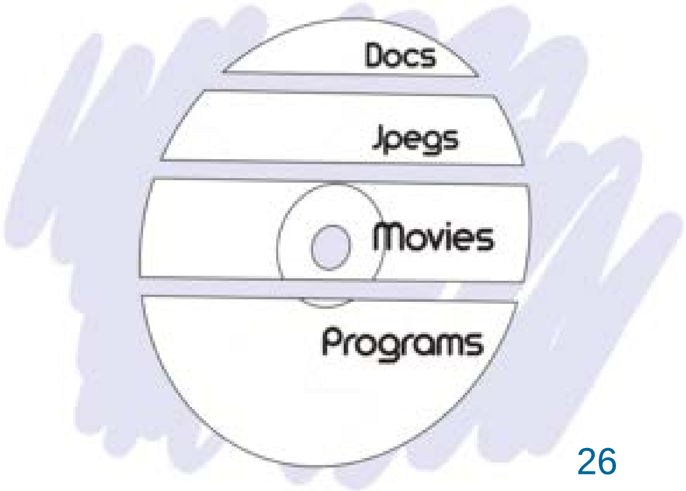
- Determining value of data
  - Spend more $$ to protect the integrity of expensive data
- Opportunity cost
- Determine when to back up data
  - Data changes frequently in most organizations
    - Constitutes daily work of users within organization
    - User data
    - Log files
    - E-mail archives

Designing a Backup Strategy

- Backup level
  - Defines how much data is backed up
  - Backup operation at given backup level stores all data that has changed since last backup of previous level
  - Levels
    - Level 0, full backup
    - Level 1, weekly differential backup
    - Level 2, daily differential backup

Designing a Backup Strategy

- Full backup
  - Also called epoch backup
  - Everything on system is backed up
- Differential backup stores only files that changed since full backup
- Incremental backup stores files that changed since most recent incremental backup or differential backup
- Separation of data for different backup options



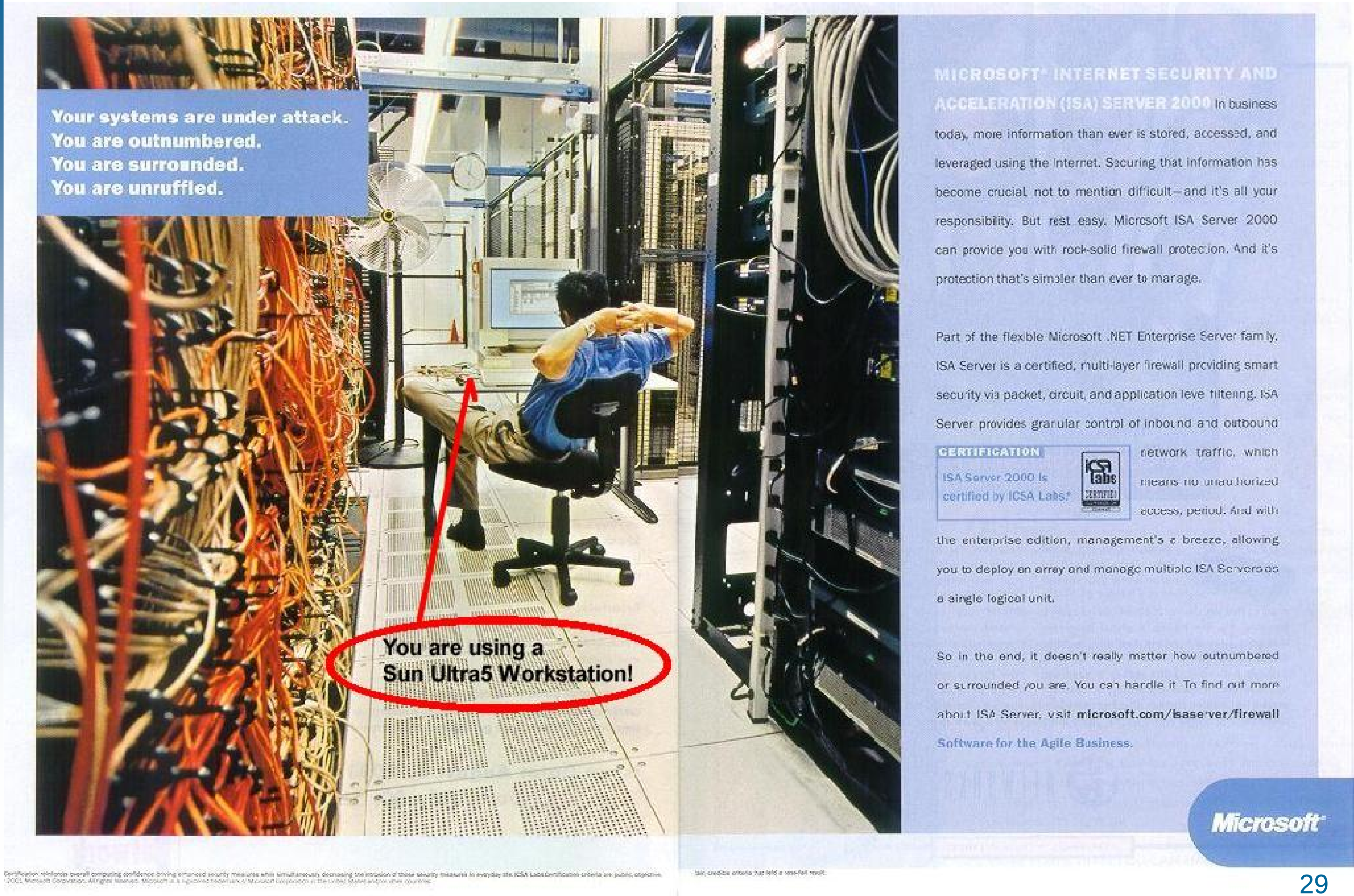
Backup

- Backed up archives should be stored in open and standard formats
  - Especially when goal is long-term archiving
  - Recovery software/hardware may have changed, and may not be available to restore data saved in proprietary formats
- System administrators and others working in the information technology field are routinely fired for not devising and maintaining backup processes suitable to their organization

Backup Events

- During a 1996 fire at the HQ of a major French bank, system administrators ran into the burning building to rescue backup tapes because they didn't have off-site copies. Data/archives were lost.
- In 2005/2006 Bank of America, Ameritrade, Citigroup, and Time Warner lost or had stolen backup tapes.
- In 2011 a software bug on Gmail caused 0.02% of the users to lose all their email. The data was restored within hours from tape backups.
  - (~400M users x 0.02% = 80,000)

Epic



Your systems are under attack.
You are outnumbered.
You are surrounded.
You are unruffled.

You are using a
Sun Ultra5 Workstation!

MICROSOFT® INTERNET SECURITY AND ACCELERATION (ISA) SERVER 2000 In business today, more information than ever is stored, accessed, and leveraged using the Internet. Securing that information has become crucial, not to mention difficult—and it's all your responsibility. But rest easy. Microsoft ISA Server 2000 can provide you with rock-solid firewall protection. And it's protection that's simpler than ever to manage.

Part of the flexible Microsoft .NET Enterprise Server family, ISA Server is a certified, multi-layer firewall providing smart security via packet, circuit, and application level filtering. ISA Server provides granular control of inbound and outbound network traffic, which means no unauthorized access, period. And with the enterprise edition, management's a breeze, allowing you to deploy an array and manage multiple ISA Servers as a single logical unit.

CERTIFICATION

ISA Server 2000 is certified by ICSA Labs.*

So in the end, it doesn't really matter how outnumbered or surrounded you are. You can handle it. To find out more about ISA Server, visit **microsoft.com/isaserver/firewall**

Software for the Agile Business.

Microsoft

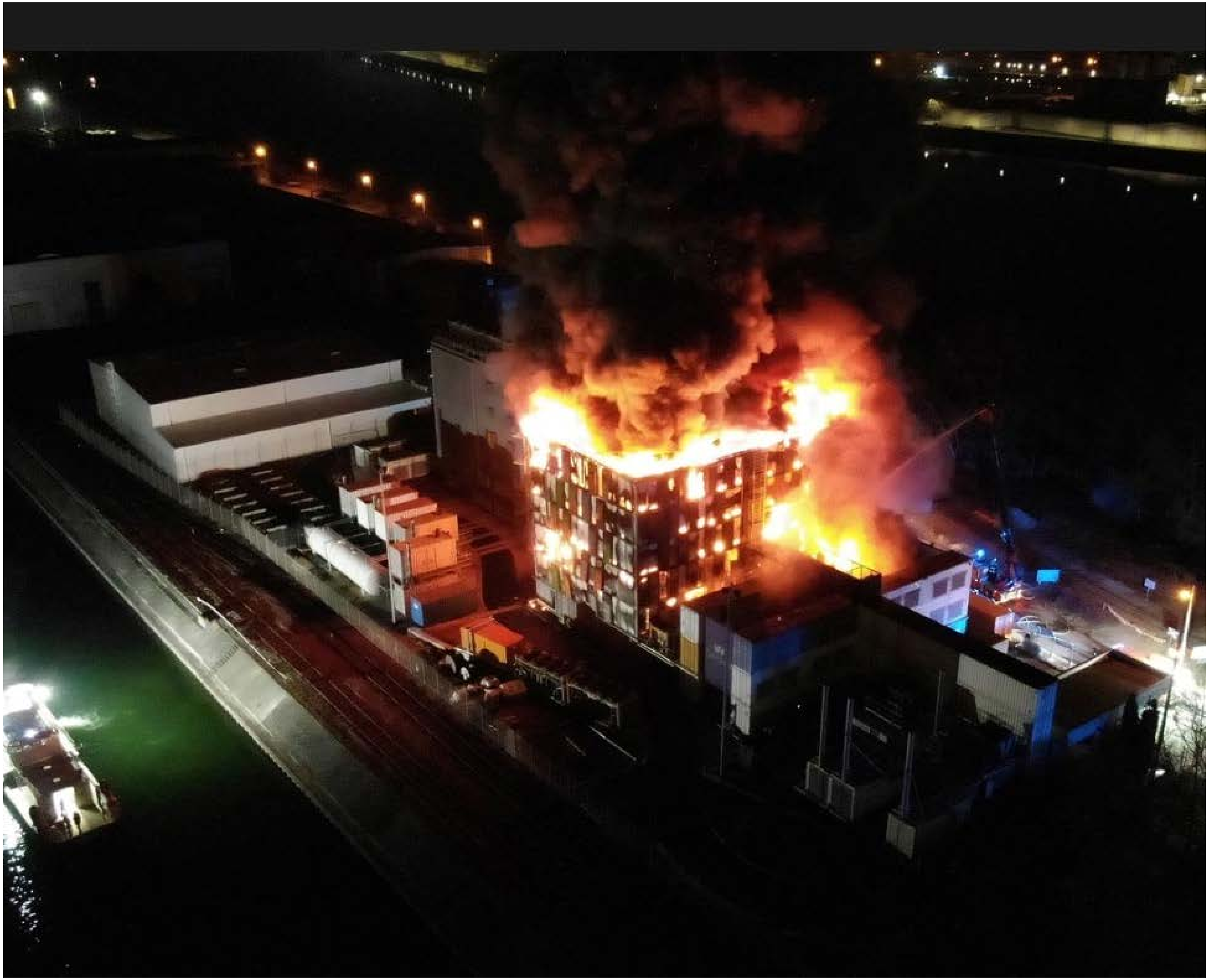
*Certification reinforces overall computing confidence driving enhanced security measures while simultaneously decreasing the intrusion of those security measures in everyday life. ICSA Labs Certification criteria are public, objective, fair, credible criteria that yield a useful result.

OVHcloud March 2021

- Millions of websites offline after fire at French cloud services firm
- Knocking out government agencies’ portals, banks, shops, game sites, news websites and taking out a chunk of the .FR web space
- No automatic fire suppression system
- No electrical cutoff mechanism
- Inner courtyard acted like fire chimneys
- Toxic fumes from lead batteries

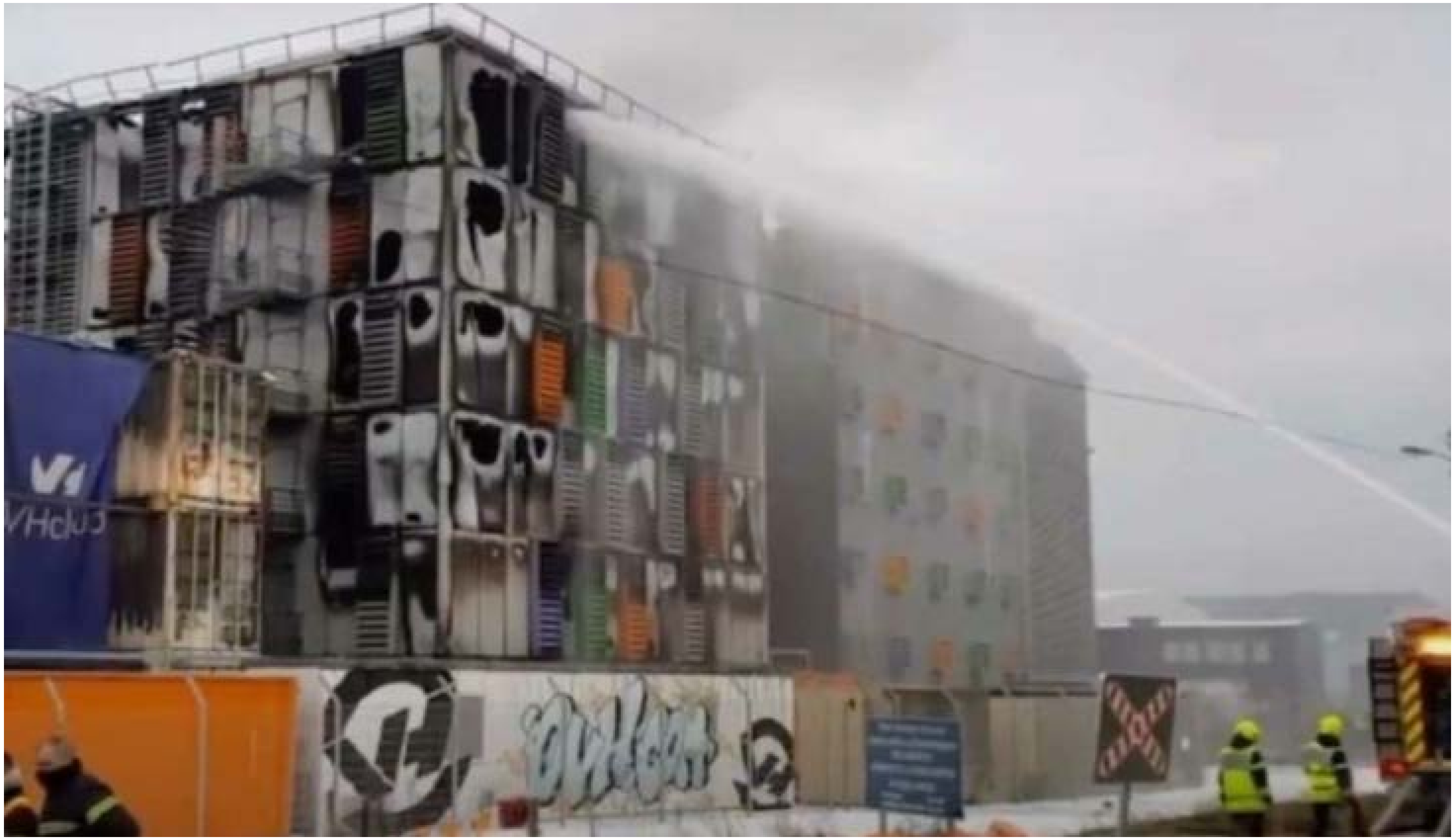
OVHcloud March 2021

OVHcloud March 2021

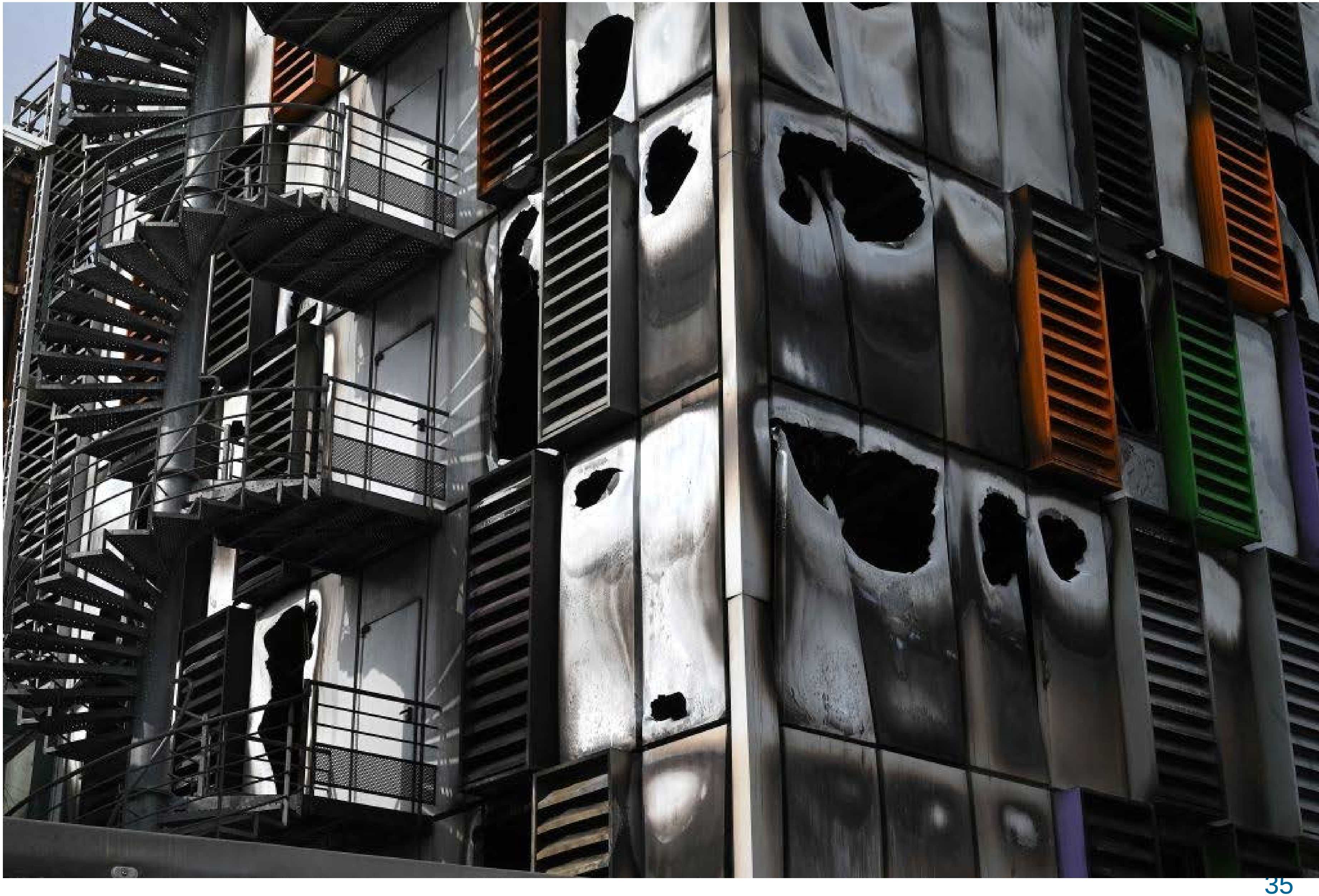


OVHcloud March 2021

OVHcloud March 2021



Built (on cheap) from shipping containers



-EOT-

CAUTION
YOU HAVE REACHED THE
LAST PAGE
OF THE INTERNET
TURN OFF YOUR BROWSER AND GO BACK TO WORK
THERE'S NOTHING ELSE TO SEE HERE