



Bacula Contra o Ransomware!

Give me my files back.

Give me \$500 in Bitcoin.



www.bacula.lat | heitor@bacula.com.br

Bacula Brasil e América Latina. All rights reserved.

Bacula LatAm



- Sede no Brasil, subsidiária nos Estados Unidos (FL)
- Distribuidor exclusivo da Bacula Systems LatAm e Brasil
- Nacionaliza licenças e serviços
- Equipe certificada pelo desenvolvedor
- Missão: *Fornecer o melhor e mais acessível Software de Backup e Restauração de Dados*



Hisense

Unimed



POUPEX

Algar
Tech



LOCAWEB



TERESINA
SHOPPING



Rio Energy

StanleyBlack&Decker

DATACOM



Binário
Cloud



UNICAMP



TRT MG
TRIBUNAL REGIONAL DO
TRABALHO DA 3ª REGIÃO



MINISTÉRIO PÚBLICO
ESTADO DE RORAIMA



MINISTÉRIO PÚBLICO
DO ESTADO DA PARAÍBA



CÂMARA MUNICIPAL DE
CAMPINAS



TRT
15ª

- Udemy.com <<http://www.bacula.lat/community/treinamento-bacula-ed/>>
- YouTube <<https://www.youtube.com/user/heitorfaria>>
- Livro Bacula 4a Edição Brasport
- Telegram: @baculabr
- Meu contato: <heitor@bacula.com.br>
- Nosso site <<http://www.bacula.lat/>>

- Ransomware
- Backups
- Bacula
- Linux
- Regra 3-2-1
- Hardening
- Perguntas e Respostas

Ransomware



De acordo com a Kaspersky [1], os Trojans Ransomware são um tipo de malware projetado para extorquir dinheiro de uma vítima. Em geral, ele vai exigir um pagamento em troca, prometendo reverter as alterações que o vírus trojan fez para o computador da vítima. Essas alterações podem incluir:

1. Criptografia de dados armazenados nas máquinas, para que as informações não possam mais ser acessadas.
2. Bloquear o acesso normal aos sistemas operacionais.



Ransomware **Attack Process**

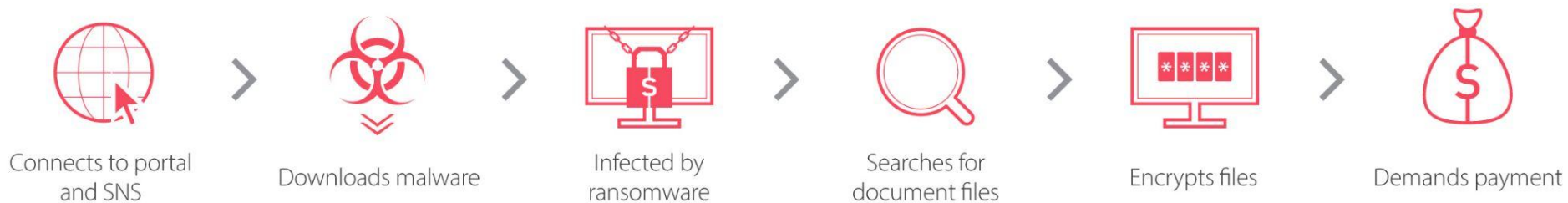


Figura 1. Processo de Ataque Ransomware

Ransomware



Figura 2. Exemplo Tela Sistema Contaminado

Ransomware



\$97,407,574.03

Total tracked ransomware payments **all time**



Figura 3. Valor total pago por rescates. Ref.: <https://ransomwhe.re/>

Ransomware



O Brasil apareceu como líder do ranking latino de ataques cibernéticos no primeiro trimestre de 2021, recebendo aproximadamente 3,2 bilhões de tentativas – quase metade da somatória de ataques recebidos na região, que chegaram à casa dos 7 bilhões. A maioria desses ataques consiste no malware conhecido como ransomware. Segundo um estudo da SonicWall Capture Labs, foi detectado um aumento de 90% dessa forma de ataques entre 2020 e 2021. Ref.: Portal it4cio

Ransomware



Striking oil

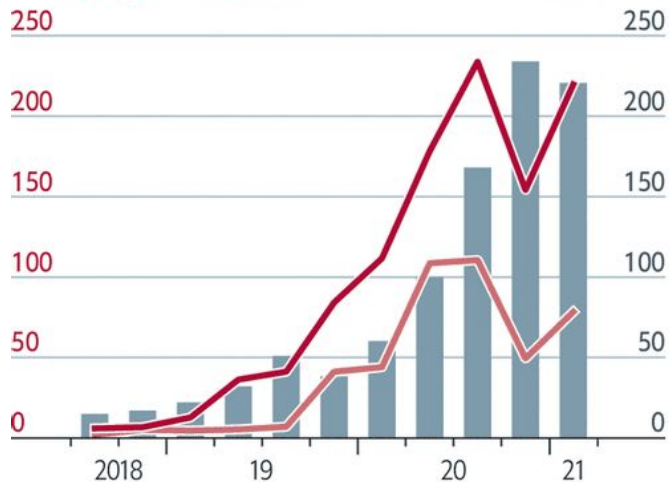
United States

Ransom payments, \$'000

— Average — Median

Median size of companies
targeted by ransomware

Employees



Sources: Coveware; Colonial Pipeline Company
The Economist

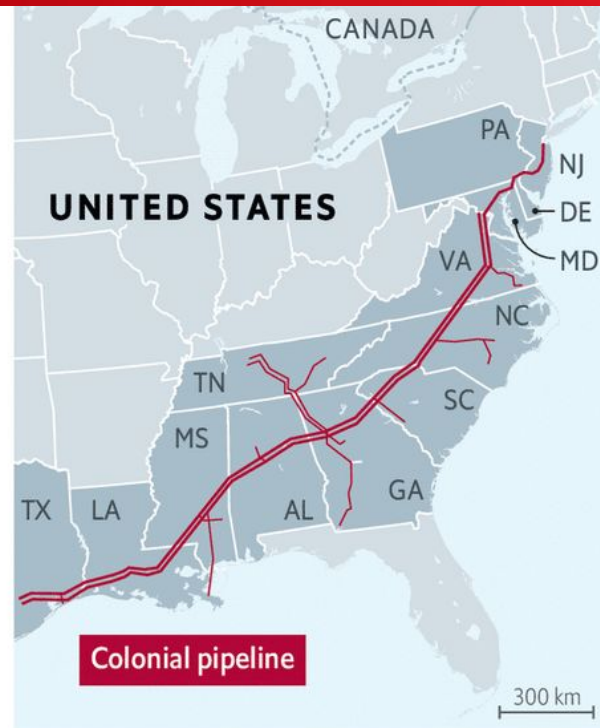


Figura 4. Evolução preço do resgate extensão do oleoduto da Colonial

Ransomware



Mesmo com seguro contra cyber ataques, pagar o resgate nem sempre é uma boa opção:

1. Sem garantia de cooperação do atacante
2. Sem garantia de funcionamento da descryptografia
3. Não mitiga novos ataques posteriores
4. Restrições de compliance e de governo (ex.: embargos governamentais contra países)
5. Moralmente questionável pois incentiva a atividade criminosa

Ransomware



1. <https://www.nomoreransom.org>



2. <https://id-ransomware.malwarehunterteam.com/>



ID Ransomware

Upload a ransom note and/or sample encrypted file to your data.

Figura 5. Sites troca de remédios.

Ransomware



Em linha com a AhnLab [2], patches de segurança e backups podem ser as únicas soluções eficazes para ataques de ransomware.

Os últimos ataques de ransomware tendem a usar novos malwares e suas variantes para burlar programas antivírus. Uma vez que é basicamente impossível preventivamente prevenir e bloquear ransomware, só podemos estabelecer uma estratégia de resposta passiva para minimizar os danos.

[2] Ransomware Response: Ideal versus

Reality. <<http://www.gartner.com/imagesrv/media-products/pdf/ahnlab/ahnlab-1-2VS6RBW.pdf>>

Ransomware



*Infelizmente, alguns fornecedores de segurança induziram os clientes a pensar que suas soluções de segurança, como programas AV, podem impedir os ransomware. No entanto, todos os fornecedores de segurança enfatizam duas medidas de segurança básicas para evitar ataques de ransomware: **fazer backup de arquivos importantes** e aplicar os patches de segurança de sistemas mais recentes.*

Em outras palavras, a aplicação dos últimos patches do sistema pode prevenir a infecção (pré-resposta) e, mesmo se ela estiver infectada, os danos podem ser minimizados ao restaurar o último backup.

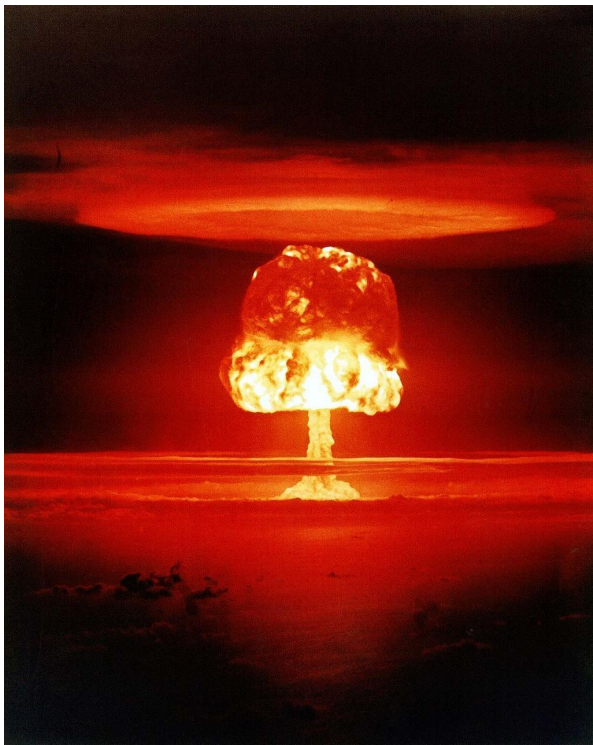


RESOLUÇÃO STJ/GP N.25

- Suspensas as atividades judicantes até 9/11
- Regime de plantão funcionará para análise de pedidos urgentes



Backups



- Redundância de dados com o propósito específico de restauração no caso de perda dos originais
- Falha de hardware; catástrofes físicas; atividade maliciosa; updates falhos de software; "eu não mexi em nada!"; update sem where; `rm -rf` errado; etc.
- Também precisa resistir ao Ransomware!

- Desde meados de 2000. **Cringe!**
- Requer Política de backup. Exemplo do Governo Federal:
*Apesar de se tratar de um controle básico, **metade das organizações respondentes (208 de 410: 50,7%) ainda não possuem tal documento. Das 202 que o elaboraram, quase metade (98 de 202: 48,5%) ainda não formalizaram essa política.***

Ref.:

<<https://portal.tcu.gov.br/imprensa/noticias/tcu-verifica-politica-de-backup-em-422-organizacoes-federais.htm>>

Backups



- 44 Zettabytes de dados a backupear em 2020
[IDC]
- Armazenamento Conjuntos de Discos, Fitas
Magnéticas Nuvem



MULTI-LEVEL DISASTER RECOVERY



BACULA

Os Três Níveis de DR

- **Nível de Dados.** Proteção dos dados de usuários e aplicações (dumps, cópia de arquivos)
- **Nível de Aplicação.** Continuidade da aplicação (PITR, CDP, plugins para aplicações)
- **Nível de SO.** Reduzir o tempo de recuperação do sistema para o menor possível (export de VM, CDP, snapshot de FS, Bare Metal)

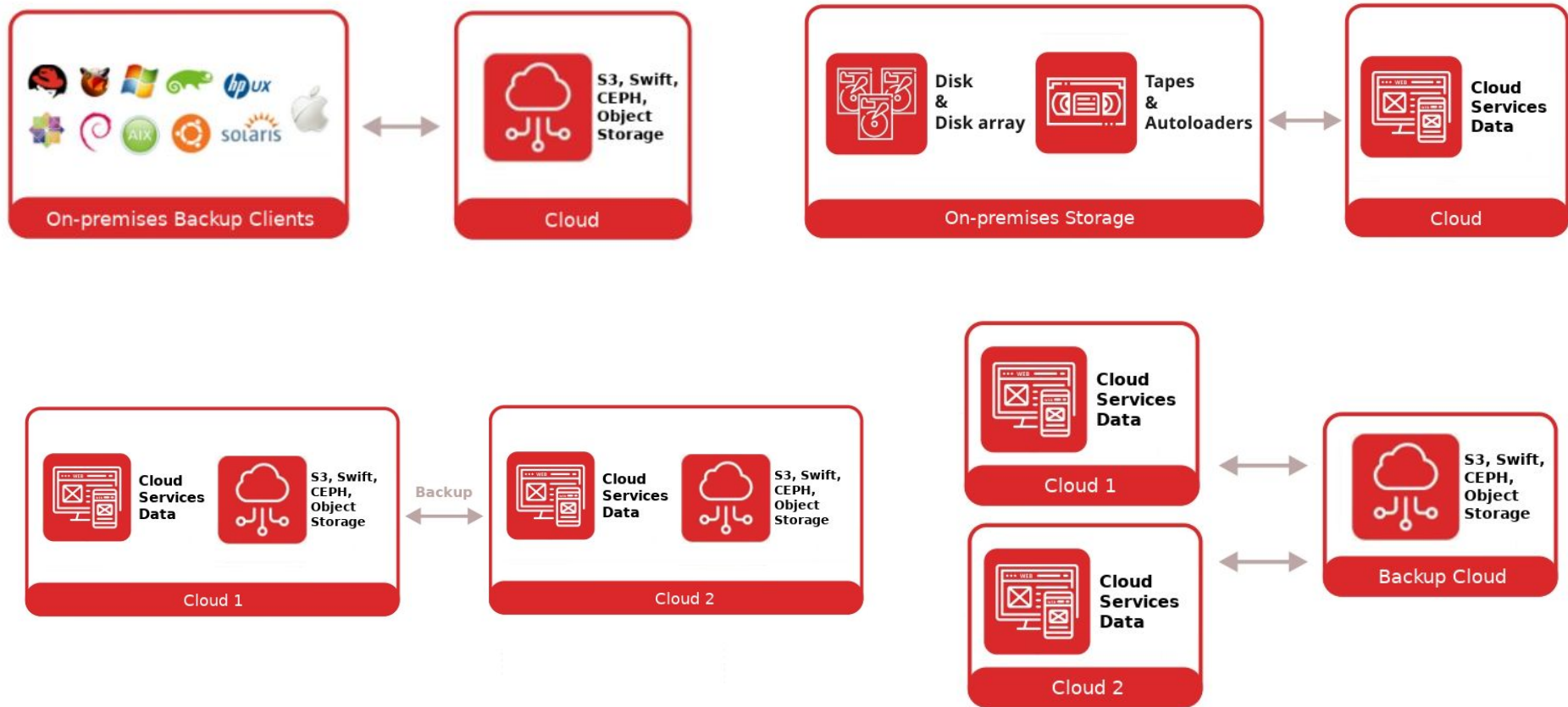


Figura 8. Principais Arquiteturas de Backup

Bacula

BACULA



Figura 9. Backup + Drácula = Bacula

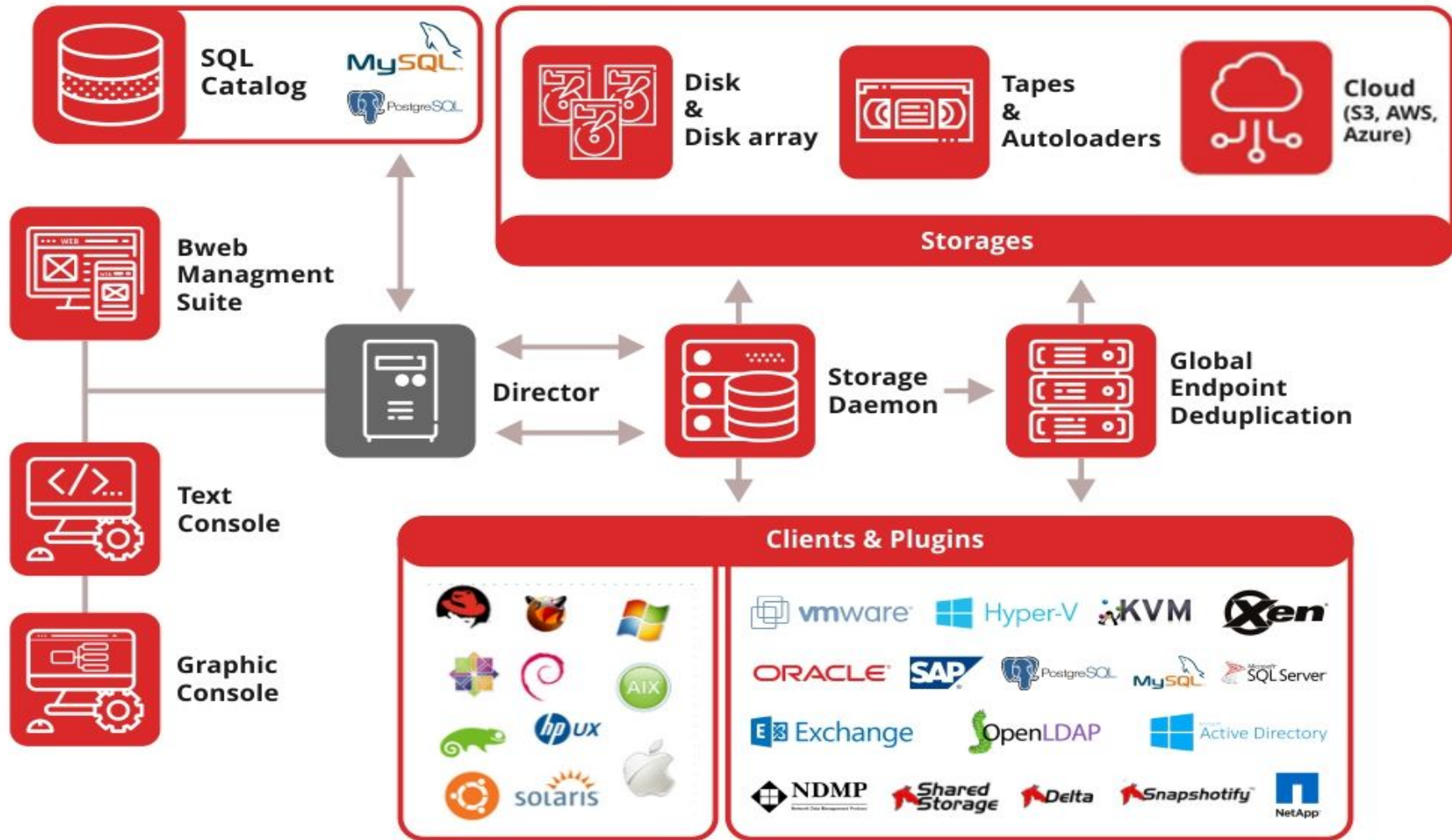
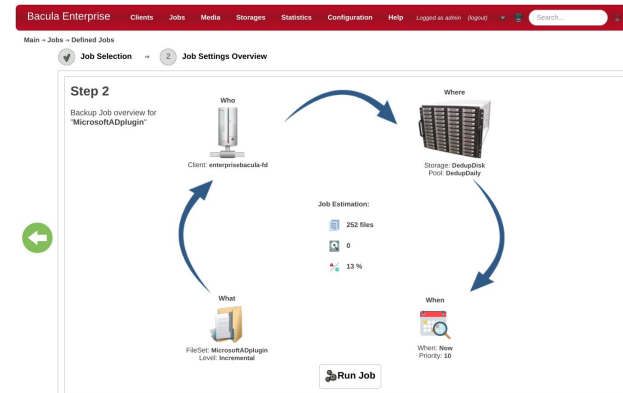


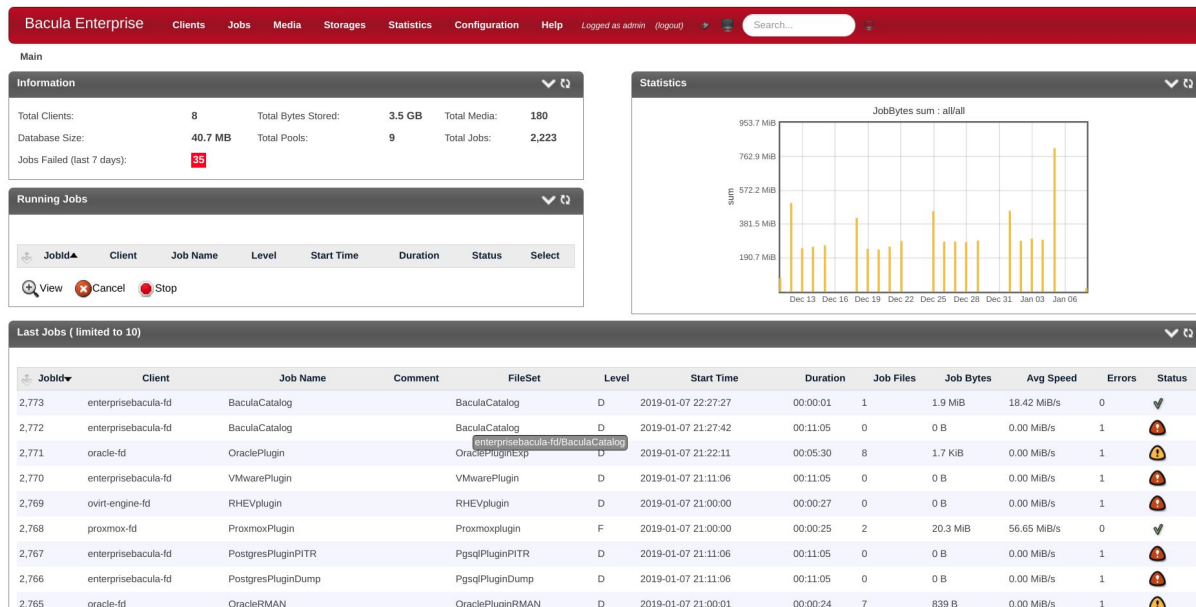
Figura 10. Arquitetura do Bacula. Também precisa ser resistente ao ransomware.

- Deduplicação Global (**na origem ou somente storage**: Windows, Unix, Linux etc.).
Até 99% de redução no tráfego e armazenamento.
- CBT para outras Virtualizações (RHV, XEN etc.)
- Primeiros Plugins para **Docker, Kubernetes, Proxmox, Hadoop, PostgreSQL e MySQL**;
- Altíssima Escalabilidade (**poucas conseguem fazer backup de 10.000 hosts ou mais**).

- Mais avançadas Interfaces Web do Mercado, sem requerer **Java/Flash**. Deploy/update remoto de agentes, etc.
- Equipe de Desenvolvimento própria
- Não é uma suíte!
- Formato de Catálogo e de Backup Abertos (sem aprisionamento);
- Versão Livre/Enterprise



- ★ Sem plugins Java/Flash
- ★ Auditoria de Operações
- ★ Self-restore
- ★ Grupos de Clientes
- ★ ACLs de Usuário e Perfis
- ★ Gestão de Mídias e Armazenamento
- ★ Módulos de Monitoração, Estatística e Relatórios
- ★ Operação dos Plugins



The screenshot displays the Bacula Enterprise BWeb interface. The top navigation bar includes 'Bacula Enterprise', 'Clients', 'Jobs', 'Media', 'Storages', 'Statistics', 'Configuration', and 'Help'. The main content area is divided into several sections:

- Information:** Shows system-wide statistics: Total Clients: 8, Total Bytes Stored: 3.5 GB, Total Media: 180, Database Size: 40.7 MB, Total Pools: 9, Total Jobs: 2,223, and Jobs Failed (last 7 days): 35.
- Running Jobs:** A table with columns for JobId, Client, Job Name, Level, Start Time, Duration, Status, and Select. It includes action buttons for View, Cancel, and Stop.
- Statistics:** A bar chart titled 'JobBytes sum : allfall' showing data from Dec 13 to Jan 06. The y-axis represents 'sum' in MB, ranging from 190.7 MB to 953.7 MB.
- Last Jobs (limited to 10):** A detailed table of recent jobs with columns: JobId, Client, Job Name, Comment, FileSet, Level, Start Time, Duration, Job Files, Job Bytes, Avg Speed, Errors, and Status.

JobId	Client	Job Name	Comment	FileSet	Level	Start Time	Duration	Job Files	Job Bytes	Avg Speed	Errors	Status
2,773	enterprisebacula-fd	BaculaCatalog		BaculaCatalog	D	2019-01-07 22:27:27	00:00:01	1	1.9 MiB	18.42 MiB/s	0	✓
2,772	enterprisebacula-fd	BaculaCatalog		BaculaCatalog	D	2019-01-07 21:27:42	00:11:05	0	0 B	0.00 MiB/s	1	⚠
2,771	oracle-fd	OraclePlugin		OraclePluginExp	D	2019-01-07 21:22:11	00:05:30	8	1.7 KiB	0.00 MiB/s	1	⚠
2,770	enterprisebacula-fd	VMwarePlugin		VMwarePlugin	D	2019-01-07 21:11:06	00:11:05	0	0 B	0.00 MiB/s	1	⚠
2,769	ovirt-engine-fd	RHEVplugin		RHEVplugin	D	2019-01-07 21:00:00	00:00:27	0	0 B	0.00 MiB/s	1	⚠
2,768	proxmox-fd	ProxmoxPlugin		Proxmoxplugin	F	2019-01-07 21:00:00	00:00:25	2	20.3 MiB	56.65 MiB/s	0	✓
2,767	enterprisebacula-fd	PostgresPluginPITR		PgsqPluginPITR	D	2019-01-07 21:11:06	00:11:05	0	0 B	0.00 MiB/s	1	⚠
2,766	enterprisebacula-fd	PostgresPluginDump		PgsqPluginDump	D	2019-01-07 21:11:06	00:11:05	0	0 B	0.00 MiB/s	1	⚠
2,765	oracle-fd	OracleRMAN		OraclePluginRMAN	D	2019-01-07 21:00:01	00:00:24	7	839 B	0.00 MiB/s	1	⚠

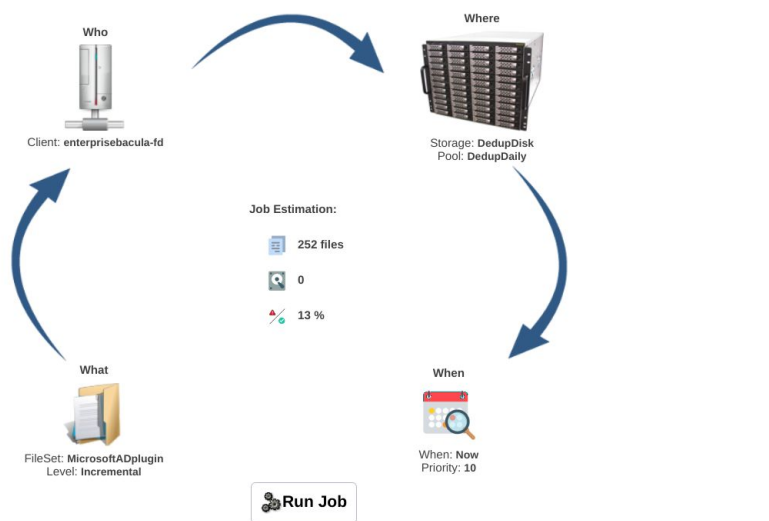
Bacula Enterprise Clients Jobs Media Storages Statistics Configuration Help Logged as admin (logout) Search...

Main → Jobs → Defined Jobs

Job Selection → 2 Job Settings Overview

Step 2

Backup Job overview for "MicrosoftADplugin"



The diagram illustrates the backup job configuration for "MicrosoftADplugin". It is divided into four quadrants: "Who" (Client: enterprisebacula-fd), "Where" (Storage: DedupDisk, Pool: DedupDaily), "What" (FileSet: MicrosoftADplugin, Level: Incremental), and "When" (When: Now, Priority: 10). A central "Job Estimation" box shows 252 files, 0 errors, and 13% progress. A "Run Job" button is located at the bottom right. Blue arrows indicate a clockwise flow between the sections.

Client: enterprisebacula-fd

Storage: DedupDisk
Pool: DedupDaily

Job Estimation:



- 252 files
- 0
- 13 %

When: Now
Priority: 10

Run Job

- ★ Operação 100% gráfica
- ★ Design Centrado no Usuário
- ★ Operações com Poucos Cliques
- ★ Integração com o AD/LDAP
- ★ Configuração e deploy de clients

Running Job OraclePlugin.2019-01-07_22:29:58_21 on oracle-fd

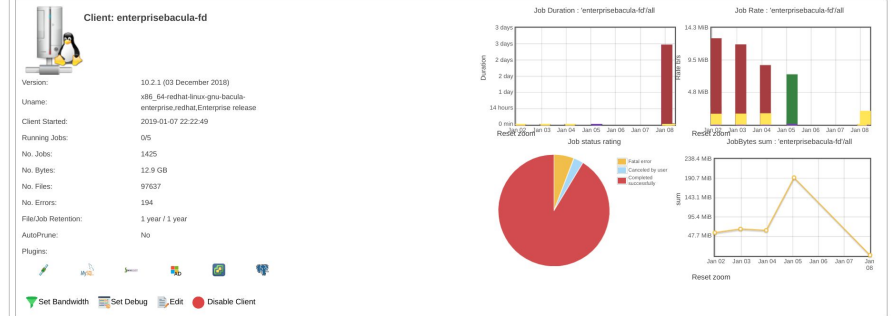
Job Name: OraclePlugin.2019-01-07_22:29:58_21 (2,774)
Processing file: /@ORACLE/cdb1\APEX_040200\user.sql
Speed: 72 B/s
Files Examined: 8
Files Backed up: 8
Bytes done: 
Files done: 
Bytes: 1,748

Job Report: OraclePlugin on oracle-fd (2774)

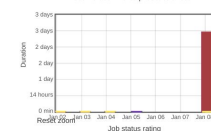
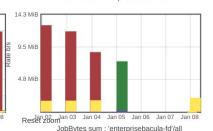
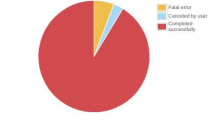
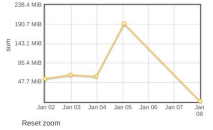
2019-01-07 22:29:50 oracle-fd JobId 2774: DIR and FD clocks differ by -9 seconds, FD automatically compensating.
 2019-01-07 22:38:00 enterprisebacula-dir JobId 2774: Start Backup JobId 2774, Job=OraclePlugin.2019-01-07_22:29:58_21
 2019-01-07 22:38:00 enterprisebacula-dir JobId 2774: Using Device "FileChgr1-Dev2" to write.
 2019-01-07 22:38:00 enterprisebacula-dir JobId 2774: FD compression disabled for this Job because AllowCompress=No in Storage resource.
 2019-01-07 22:38:00 enterprisebacula-sd JobId 2774: Volume "dedupDaily-74" previously written, moving to end of data.
 2019-01-07 22:38:00 enterprisebacula-sd JobId 2774: Ready to append to end of Volume "dedupDaily-74" size=1,922,059

Main - Clients - Client Status enterprisebacula 3 minutes

Client: enterprisebacula-fd



Version: 10.2.1 (03 December 2018)
Uname: x86_64-redhat-linux-gnu-bacula-enterprise-redhat.Enterprise release
Client Started: 2019-01-07 22:22:49
Running Jobs: 0/5
No. Jobs: 1425
No. Bytes: 12.9 GB
No. Files: 97637
No. Errors: 194
FileJob Retention: 1 year / 1 year
AutoPrune: No
Plugins:

Job Duration: 'enterprisebacula-fd' 
Job Rate: 'enterprisebacula-fd' 
Job Status Rating: 
Jobilities sum: 'enterprisebacula-fd' 

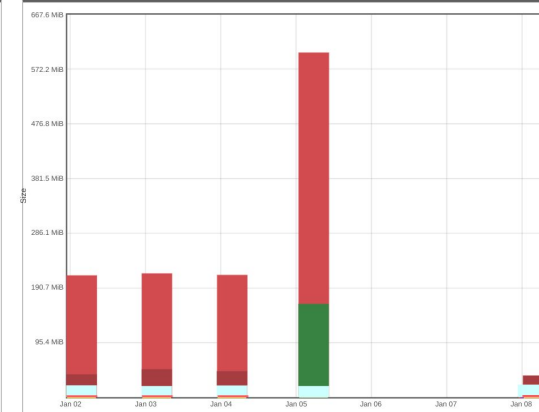
Running Jobs
 No job running on the Client.
Terminated Jobs

Main - Statistics - Statistics

Options

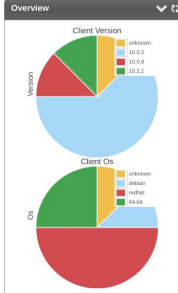
Level: Any **Status:** OK
Age: This week **Size:** Width: 800 Height: 600
Clients: enterprisebacula-fd, hyper-fd, mssql-fd, oracle-fd, ovirt-engine-fd, proxmox-fd, test, test-fd
Job Name: BackupImages, BackupVideo, BaculaAdminTask, BaculaAudio, BaculaCatalog, BaculaConfigurations, BaculaFileCompressor, HypervPlugin, LDAPPlugin, MicrosoftADplugin, mssqlBacula, MSSQLPluginCluster, MySQLplugin, NewJob, OraclePlugin

Groups: databases, hypervisors

Current graph


Main - Clients - Clients

Overview



Client Version: 10.2.1, 10.1.8, 10.2.2
Client OS: Unknown, Debian, Oracle, S4.12

Clients

Name	Select	Desc	Auto Prune	File Retention	Job Retention
enterprisebacula-fd	<input type="checkbox"/>	10.2.1 (03Dec18) x86_64-redhat-linux-gnu-bacula-enterprise-redhat.Enterprise release	0	365 days	365 days
hyper-fd	<input type="checkbox"/>	10.0.2 (30May18) Microsoft (build 9200), 64-bit,Cross-compile,Win64	0	365 days	365 days
mssql-fd	<input type="checkbox"/>	10.0.8 (22Oct18) Microsoft (build 9200), 64-bit,Cross-compile,Win64	0	365 days	365 days
oracle-fd	<input type="checkbox"/>	10.0.2 (30May18) x86_64-redhat-linux-gnu-bacula-enterprise-redhat,	0	365 days	365 days
ovirt-engine-fd	<input type="checkbox"/>	10.0.2 (30May18) x86_64-redhat-linux-gnu-bacula-enterprise-redhat,	0	365 days	365 days
proxmox-fd	<input type="checkbox"/>	10.0.2 (30May18) x86_64-pc-linux-gnu-bacula-enterprise,debian.9.0	0	365 days	365 days
test	<input type="checkbox"/>	10.0.2 (30May18) x86_64-pc-linux-gnu-bacula-enterprise,debian.9.0	0	365 days	365 days
test-fd	<input type="checkbox"/>	10.0.2 (30May18) x86_64-redhat-linux-gnu-bacula-enterprise-redhat,	0	365 days	365 days

Edit Fileset VMwarePlugin

Fileset Name: VMwarePlugin

Description:

Enable VSS:

Ignore Fileset Changes:

Enable Snapshot:

Include: [Compression Dedup Signature] Plugin: index

Exclude:

VMware resource browser

Path: /ha-datacenter/VMS

- [-] .
- [-] ..
- [-] centos7minimum
- [-] teste-restore

Buttons: Cancel, Save, Copy, Delete, Add Include list

Storage Overview

Storage: DedupDisk Refresh: 30 seconds

Legend: Queued (red), Progress (green), Done (gray), Error (black), Cancelled (yellow), Unknown (light green)

Device: Single Device

Uploads: No upload transfer available

Downloads: No download transfer available

Device Name	Status	Loaded	Volume Name	Slot	Running Jobs/Max. Jobs	Speed
AWS						
Device Details: Device Type: Cloud, Media Type: CloudAWS, Device Status: Not running (Idle), Cache (Free/Total): 272.81 GB / 369.98 GB, Status: Cloud Status						
Autochanger: FileChgr1						
Device Details: Device Type: Dedup, Media Type: Dedup, Device Status: Not running (Idle), Space (Free/Total): 272.81 GB / 369.98 GB						
FileChgr1-Dev1	-	-	-	05	-	-
FileChgr1-Dev2	-	-	-	05	-	-
Autochanger: FileChgr2						
Device Details: Device Type: File						

Main - Statistics - Dedup Usage

Global Endpoint Deduplication storage usage

Storage: DedupDisk Refresh interval: 5 minutes

Deduplication Ratio:

Ref ratio: 6.63

Size ratio: 14.13

General:

Version: 10.3

Hash Name: sha512/256

Hash ID: 1

Hole Size: 4.0 MB

Ideal Blocksize: 64.0 KiB

Max Blocksize: 65.0 KiB

Statistics:

Transaction: 2476

Hash Count: 1,205,527

Ref Count: 7,994,509

482.8 GiB

Dedupengine Errors: 0

Containers Errors: 0

Containers statistics:

Chunk Used: 1,205,527

Chunk Allocated: 1,889,390

Disk Space Used: 34.2 GiB

Disk Space Allocated: 71.4 GiB

Container Sum Bitarray Capacity: 33.0 MB

Read Chunk: 0

Calc Hash: 784

Update Refont: 0

Query Hash: 2138

New Hash: 681

Vacuum:

Start Time: 2018-10-29 17:14:48

End Time: 2018-10-29 17:14:55

Orphan Addr: undefined

Ref Count: 0

Ref Size: 0 B

34.2 GiB Actual disk space used, 482.8 GiB Equivalent standard File or Tape storage space

Global Endpoint Deduplication storage containers

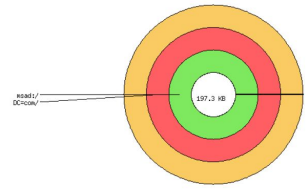
ID#	Block Used	Block Capacity	Unused Disk Space	Disk Space	Bitarray Capacity	Usage	Usage Map
1	3	4	1024 B	8.0 KiB	524288	75%	[Progress bar]
2	6,483	9,551	6.0 MiB	18.7 MiB	524288	67%	[Progress bar]
3	10,941	13,774	6.3 MiB	40.4 MiB	524288	79%	[Progress bar]
4	10,628	12,865	8.7 MiB	50.3 MiB	524288	82%	[Progress bar]
5	5,574	7,063	7.3 MiB	34.5 MiB	524288	78%	[Progress bar]

JobID	Client	Job Name	Comment	FileSet	Level	Start Time	Duration	Job Files	Job Bytes	Avg Speed	Errors	Status
2,784	enterprisebacula-td	MicrosoftADplugin		MicrosoftADplugin	F	2019-01-07 23:37:41	00:00:02	252	169.8 KiB	0.10 MiB/s	0	✓

Buttons: Delete, View Media, View Jobs, View Stats, View FileSet, View Usage, View File List, Run Again, Restore, Edit, Verify Data

Files usage

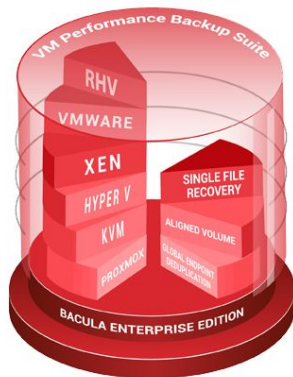
/ Size go go back



Plugins



- VMware
- Hyper-v
- KVM
- Xen
- Proxmox
- RHEL/oVirt
- Nutanix



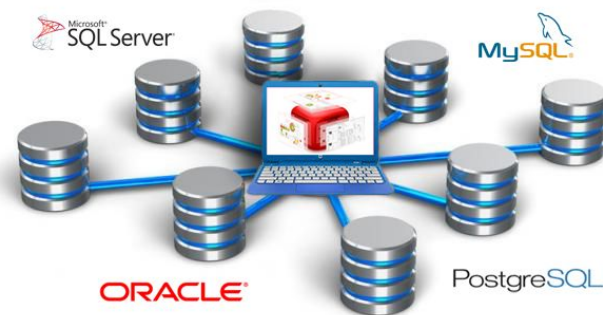
- ★ Backup sem Cliente
- ★ Auto-Descoberta de Novas Máquinas
- ★ Backup Diferencial no Nível de Bloco
- ★ Restauração Automática de VMs
- ★ Restauração granular de um arquivo
- ★ Instant Recovery

Plugins



- MYSQL
- PostgreSQL
- Oracle DB
- SAP
- SAP Hana
- Sybase ASE
- MS SQL
- Active Directory
- LDAP
- MongoDB
- Hadoop
- DB2
- Cassandra*

- ★ Auto-Descoberta de Novos Bancos
- ★ Backups Diferenciais e Incrementais
- ★ PITR / Archive Log
- ★ Restauração Granular e Automática
- ★ Backup de Clusters



Plugins



- CDP (replicação de arquivo e VMs*)
- Docker, Kubernetes, OpenShift
- Hadoop
- Bare Metal Linux e Windows
(restauração e migração de máquinas completas físicas/virtuais/nuvem)
- Zimbra, MS Exchange
- Sharepoint
- VSS
- Office 365
- Snapshot Linux
- bpipe
- Delta
- NDMP
- Shared Storage SAN
- Incremental Netapp
- Cloud (Oracle, Amazon Glacier, Google, Azure, Swift e S3)



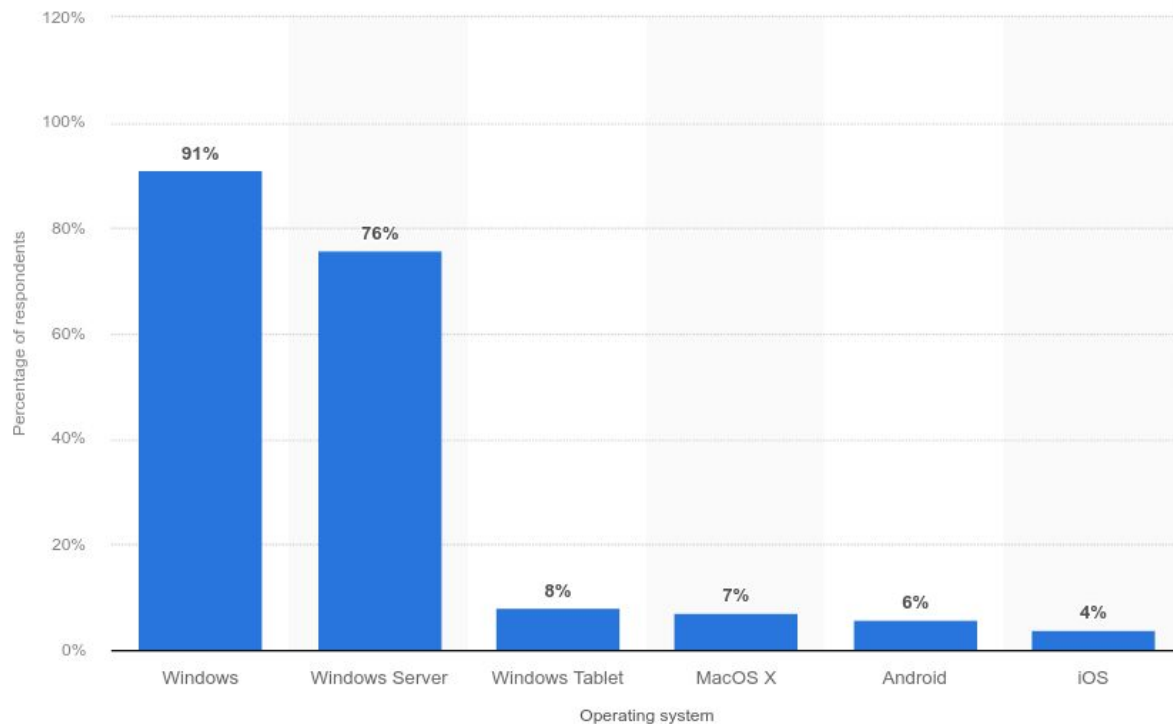


Figura 11. SOs que Usuários Reportaram Contaminação de Ransomware

1. In 2021, 100% of the world's top 500 supercomputers run on Linux.
2. Out of the top 25 websites in the world, only 2 aren't using Linux.
3. 96.3% of the world's top 1 million servers run on Linux.
4. 90% of all cloud infrastructure operates on Linux and practically all the best cloud hosts use it.

Ref.: <<https://hostingtribunal.com/blog/linux-statistics/>>



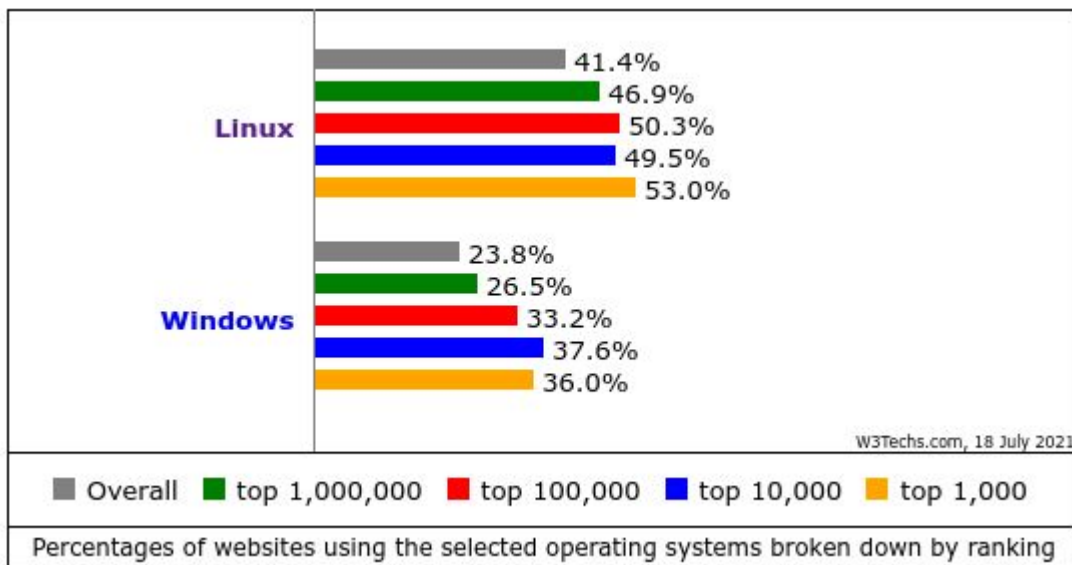


Figura 11. SO de Servidores WEB. Ref.:

<<https://w3techs.com/technologies/comparison/os-linux,os-windows>>

- ★ Bacula é pioneiro no Servidor primariamente em Linux, dentre os Líderes
- ★ Maior quantidade de plataformas Clientes, incluindo Windows, Mac OS, Linux, Unix, Android etc.



Figura 11. Clientes de Backup suportados pelo Bacula

Regra 3-2-1



Using tape backup as part of an overall data management strategy allows use to follow best practices in data backup and compliance, specifically the widely known 3-2-1 rule, which is:

1. Maintain three separate copies of your data.
2. Store your data on at least two different types of storage media.
3. Keep one copy of your data in an off-site location.

Ref.:

<<https://searchstorage.techtarget.com/IronMountainCloud/A-New-Old-Weapon-Against-Ransomware-Tape-Backup>>

Regra 3-2-1



- Suporte nativo desde a concepção de gravação direta em todas as fitas, cartuchos, VTL etc.
- Primeira a suportar driver de armazenamento em múltiplos provedores de Object Storage (**S3**, **Glacier**, **Oracle**, **Google**, **Azure**, **Swift** etc.).



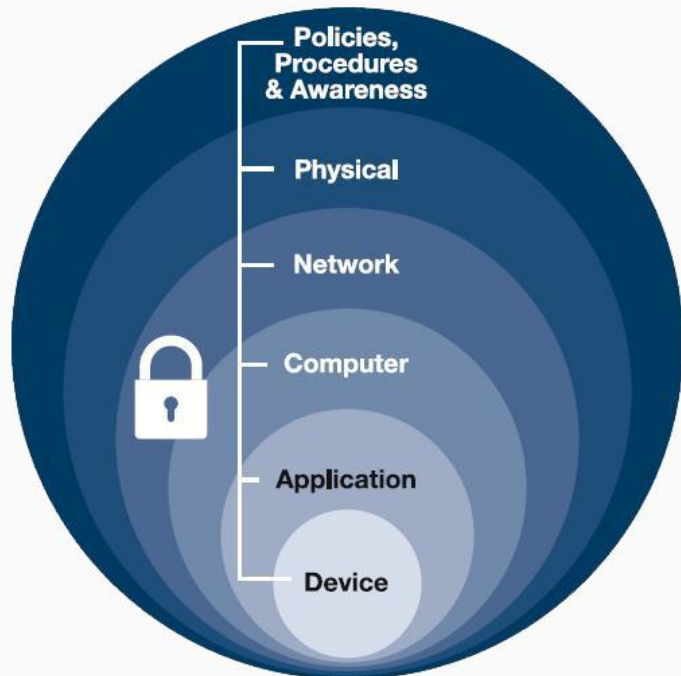
Figura 12. Plugins de Nuvem do Bacula

Hardening



Systems hardening is a collection of tools, techniques, and best practices to reduce vulnerability in technology applications, systems, infrastructure, firmware, and other areas. The goal of systems hardening is to reduce security risk by eliminating potential attack vectors and condensing the system's attack surface. By removing superfluous programs, accounts functions, applications, ports, permissions, access, etc. attackers and malware have fewer opportunities to gain a foothold within your IT ecosystem.

Ref.: <<https://www.beyondtrust.com/resources/glossary/systems-hardening>>



- ★ Protocolos de conexão socket exclusivos e nunca violado. Todas comunicações criptografadas automaticamente com certificado FIPS.
- ★ Apenas o usuário bacula do sistema de arquivos precisa ter acesso de escrita nos volumes de backup em disco, fita, nuvem e catálogo de backup.
- ★ **Volumes Imutáveis**
- ★ **Backup Poisoning Detection**
- ★ **Virus Detection**

Hardening



- ★ Backup Regular do Catálogo
- ★ Catálogo remoto / em outra máquina / PaaS (ex. Oracle OCI MySQL, Heroku/Aiven PgSQL etc.)
- ★ Cluster



Hardening



```
[root@enterprisebacula ~]# ls -lah /mnt/dedup/Dedup*  
-rw-r----- 1 bacula disk 4,7M Mai 4 18:01 /mnt/dedup/DedupArchive-0  
-rw-r----- 1 bacula disk 4,7M Mai 4 19:37 /mnt/dedup/DedupArchive-2-49  
-rw-r----- 1 bacula disk 4,8M Mai 4 19:47 /mnt/dedup/DedupArchive-2-50  
-rw-r----- 1 bacula disk 4,6M Mai 4 19:53 /mnt/dedup/DedupArchive-2-51  
-rw-r----- 1 bacula disk 4,2M Mai 4 20:10 /mnt/dedup/DedupArchive-2-52  
-rw-r----- 1 bacula disk 4,7M Mai 4 17:52 /mnt/dedup/DedupArchive-47  
-rw-r----- 1 bacula disk 14M Jun 8 11:11 /mnt/dedup/DedupDaily-0  
-rw-r----- 1 bacula disk 3,1M Jun 3 15:39 /mnt/dedup/DedupDaily-1  
-rw-r----- 1 bacula disk 215M Mai 4 15:37 /mnt/dedup/DedupDaily-10  
-rw-r----- 1 bacula disk 5,9M Mai 6 11:11 /mnt/dedup/DedupDaily-11  
-rw-r----- 1 bacula disk 5,0M Abr 6 11:10 /mnt/dedup/DedupDaily-12  
...
```

- ★ Possibilidade de imutabilizar e indeletabilizar os volumes de backups em disco ou em nuvem encerrados para gravação. Ex. disco:

```
# Seta o atributo imutável e não-deleção no volume de disco:  
chattr +iu <volume_bacula>
```

```
# Remove o atributo imutável e não-deleção no volume de disco:  
chattr -iu <volume_bacula>
```

```
# Arquivo sem flag de imutabilidade e indeletabilidade:
```

```
hfaria@hfaria-P65:/tmp$ lsattr arq
```

```
-----e----- arq
```

```
# Arquivo com flag de imutabilidade:
```

```
hfaria@hfaria-P65:/tmp$ lsattr arq
```

```
-u--i-----e----- test arq
```

```
# Nesse estado nem o root pode alterar!
```

```
hfaria@hfaria-P65:/tmp$ sudo echo dados > arq
```

```
bash: arq: Operation not permitted
```

Hardening



```
#!/bin/bash
# Remove imutabilidade todos arquivos diretório, ex. Job Admin
/opt/bacula/scripts/imut_tira.sh (pré-jobs diários)
for filename in /mnt/backup/*; do
    chattr -i $filename
done

#!/bin/bash
# Adiciona imutabilidade e indeletabilidade todos arquivos diretório,
ex. Job Admin /opt/bacula/scripts/imut_poe.sh (pós-jobs diários)
for filename in /mnt/backup/*; do
    chattr +iu $filename
done
```

Hardening



- ★ [LTO-9] With 18 TB of raw and up to 45 TB* of compressed capacity, and a full-height drive performance of up to 1000 MB/sec (3.6 TB/Hr.)
Ref.: <https://www.quantum.com/en/products/tape-storage/lto-9/>
- ★ Esquema GFS com Pool Off-site. Ou uso de fitas WORM (Ref.: <https://techmonitor.ai/techonology/data/could-worm-help-build-local-govt-resilience-to-ransomware>).
- ★ Trava Manual Read-Only

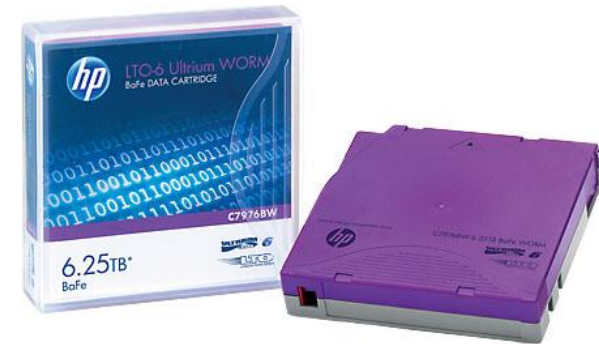


Figura 14. Foto de Fita WORM LTO-6

Perguntas e Respostas





www.bacula.com.br

heitor@bacula.com.br

Diretoria Comercial

Melissa Faria – melissa@bacula.com.br