Symantec NetBackup Blueprints

Blueprint for NetBackup Security in 7.6

Symantec Backup and Recovery Technical Services

Notice

This NetBackup Blueprint presentation includes example diagrams that contain objects that represent applications and platforms from other companies such as Microsoft and VMware. These diagrams may or may not match or resemble actual implementations found in end user environments. Any likeness or similarity to actual end user environments is completely by coincidence.

The goal of the diagrams included in this blueprint presentation is not to recommend specific ways in which to implement applications and platforms from other companies such as Microsoft and VMware; the purpose of these diagrams is to illustrate NetBackup best practices only.

For guidelines and best practices on installing and configuring applications and platforms from other companies, please refer to best practice documentation and other resources provided by those companies.

FEEDBACK

Please hide this slide before presenting. For Internal Use only.

To provide Feedback and Rate this document, please use the FEEDBACK LINK.

Note: You must be in Slide Show mode to make the link clickable.

This link will redirect you to Google Forms.

Thank you

Symantec NetBackup Blueprints
How to use ?

These **Blueprints** are designed to show customer challenges and how NetBackup solves those.

- Each Blueprint consists of:
  - **Pain Points**: Explain the current challenges a customer faces.
  - **Whiteboards & Example Diagrams**: Describe the implementation of NetBackup solution.
  - **Best Practices**: Present NetBackup best practices to avoid common pitfalls
- Use these **Blueprints** to present the NetBackup best practice implementation example

Pain Points

Present-day challenges

- Software security is extremely crucial to prevent a hacking attempt.
- Network intrusion or hacking causes downtime, loss of data and revenue, damages the brand image, and can lead to legal issues.
- Software security assurance needs to be addressed holistically and systematically in the same way as quality and safety.
- Sensitive data backed up to tape needs to be encrypted to safeguard against misuse, compromise, and loss.
- Unified Security to manage heterogeneous backup environments.

NetBackup Advantages

About NetBackup security and encryption

- NetBackup Security and Encryption protect all NetBackup operations on NetBackup master servers, media servers, and attached clients.
- Backed up data is protected through Encryption and vaulting.
- NetBackup data that is sent over the network is protected through dedicated and secure network ports.

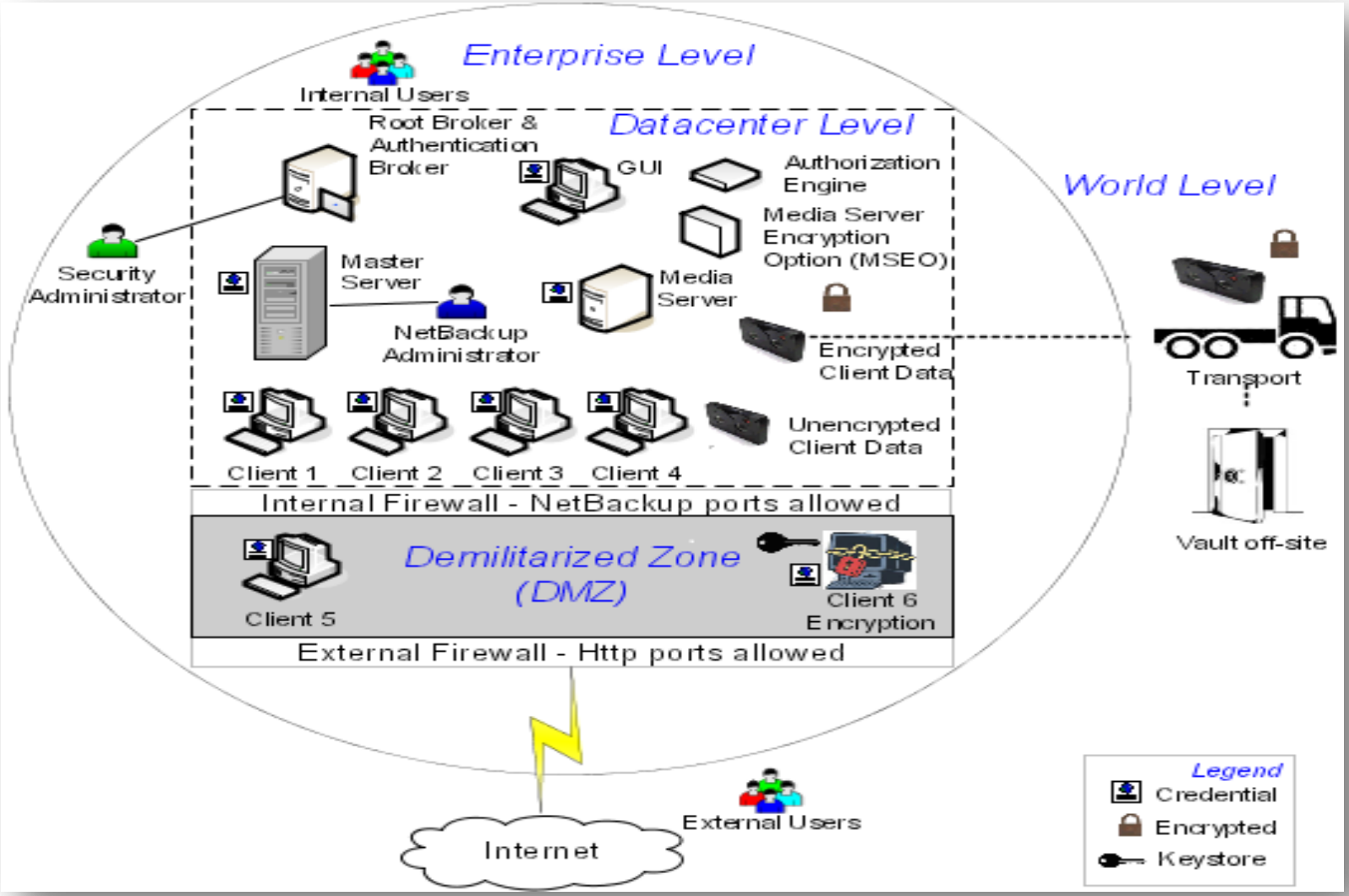
NetBackup security implementation levels

Security level	Description
World level Security	Lets external users access corporate Web servers behind firewalls. Also allows encrypted tapes to be transported and vaulted off site. It encompasses the enterprise level and the datacenter level. For more information , click the following link: http://www.symantec.com/docs/HOWTO46725
Enterprise level Security	It has tangible parts of the NetBackup security implementation. It encompasses internal users, security administrators, and the datacenter level. For more information ,click the following link : http://www.symantec.com/docs/HOWTO46726
Data centre level Security	Data centre level Security can consist of a workgroup, a single datacenter, or a multi-datacenter. For more information ,click the following link: http://www.symantec.com/docs/HOWTO46727

NetBackup components that can be secured.

Component	Description
Master and Media server security	The authentication broker provides credentials to the master server and the media server. This is done to limit access to portions of NetBackup.
Operating System security	Operating system security can be enhanced for master servers, media servers and clients.
Client security	Data is encrypted on the client. Encrypted data is sent over the wire.

NetBackup Blueprints: Security
Combined world, enterprise, and datacenter levels



This can be enhanced for master servers, media servers, and clients by performing the following tasks

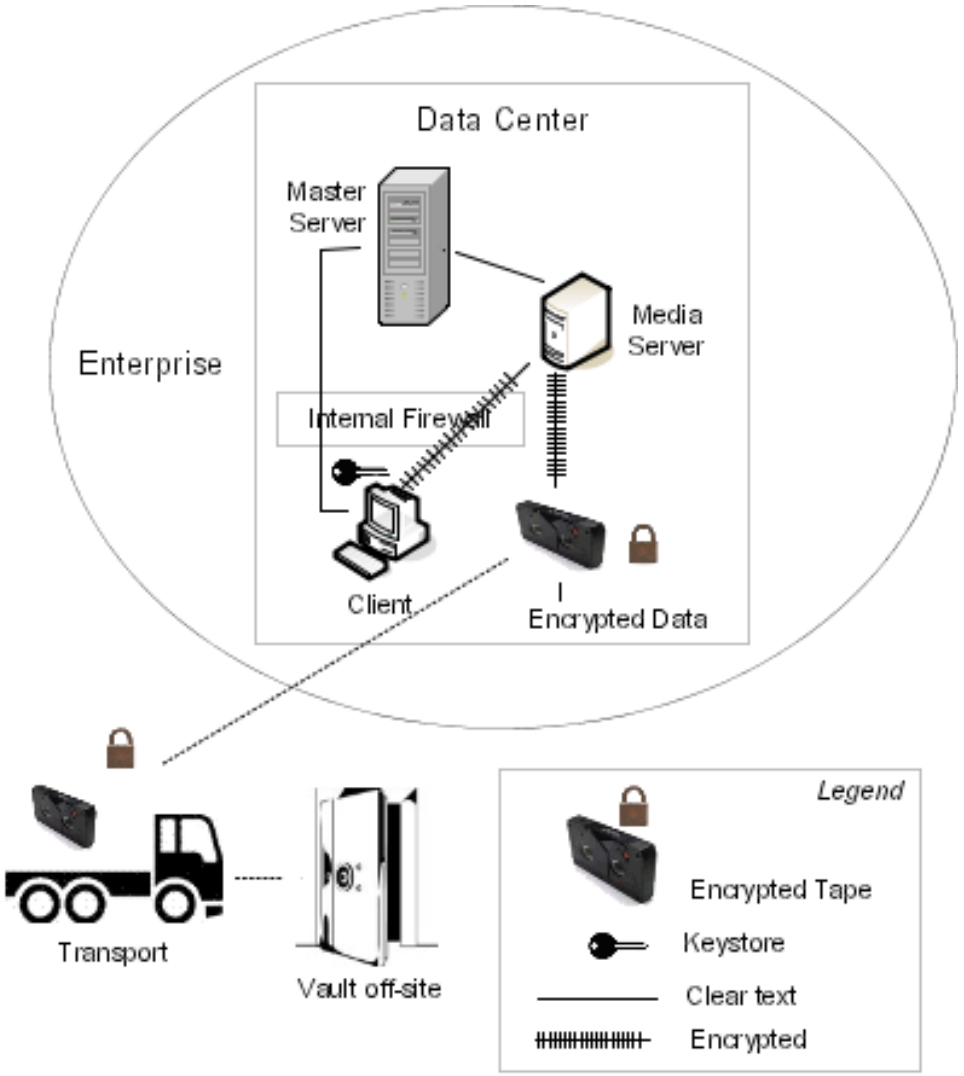
- Installing OS patches. These include updates and upgrades. They have to be at a level specified by the vendor.
- Following safe firewall procedures.
- Employing least privilege administration.
- Limiting root users.
- Applying security protocol over IP (IPSEC) hardware.

For more information , refer to the following article:

http://www.symantec.com/docs/HOWTO46721

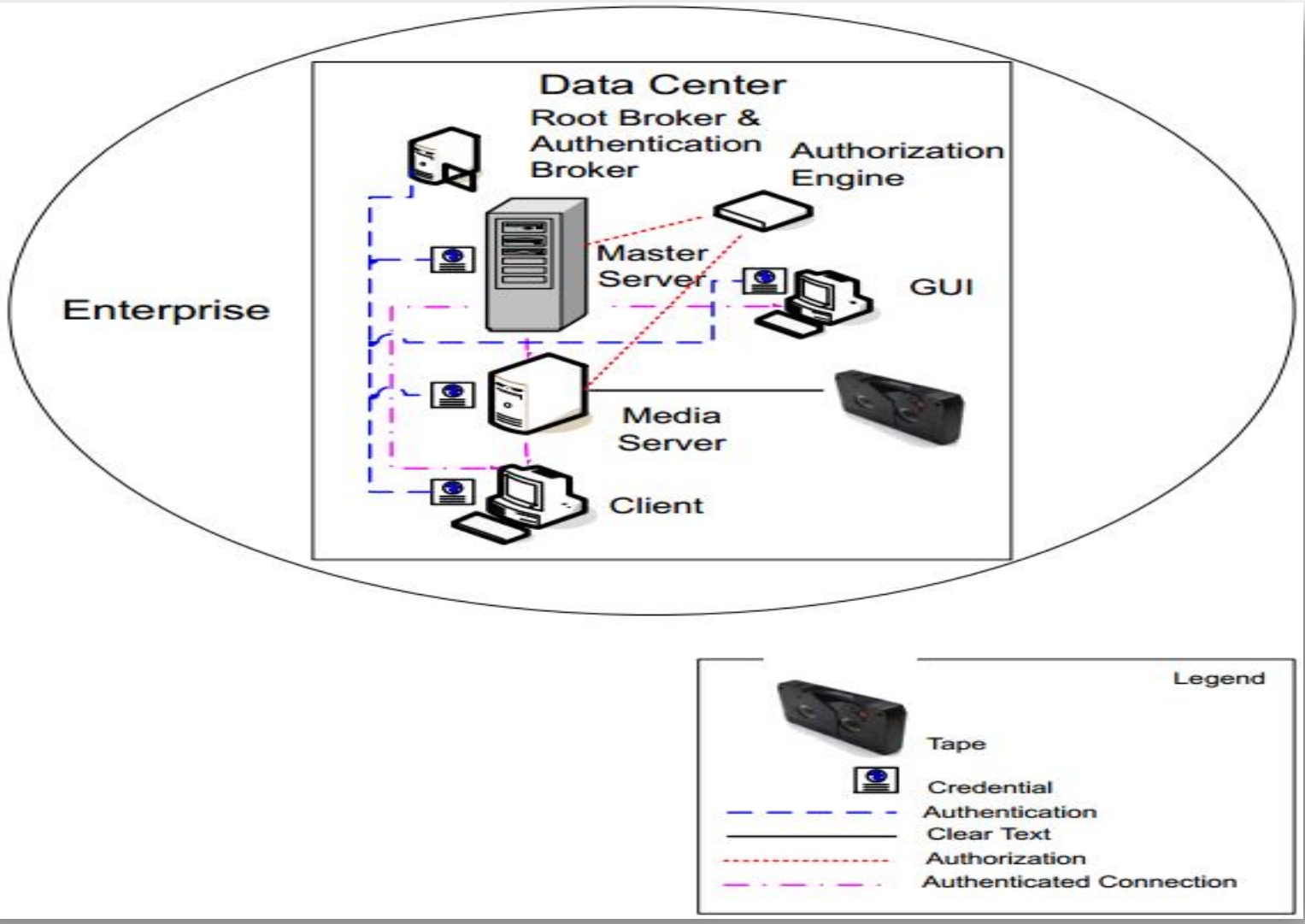
Standard NetBackup Security

- Standard NetBackup security only includes security provided by the OS and the hardware components of the datacenter.
- Client data is not encrypted. The master server, media server, and client are all run within the local enterprise datacenter
- Storing unencrypted data on-site poses a high risk for the DR plan. Data sent off-site, if intercepted, could compromise confidentiality



- This method uses authentication broker to provide credentials to the master server, media server, and client.
- This environment is very similar to the NBAC master, media server, and GUI model.
- Main difference is that all hosts are reliably identified using credentials
- User identities can exist in global repositories such as AD in Windows or NIS in UNIX.

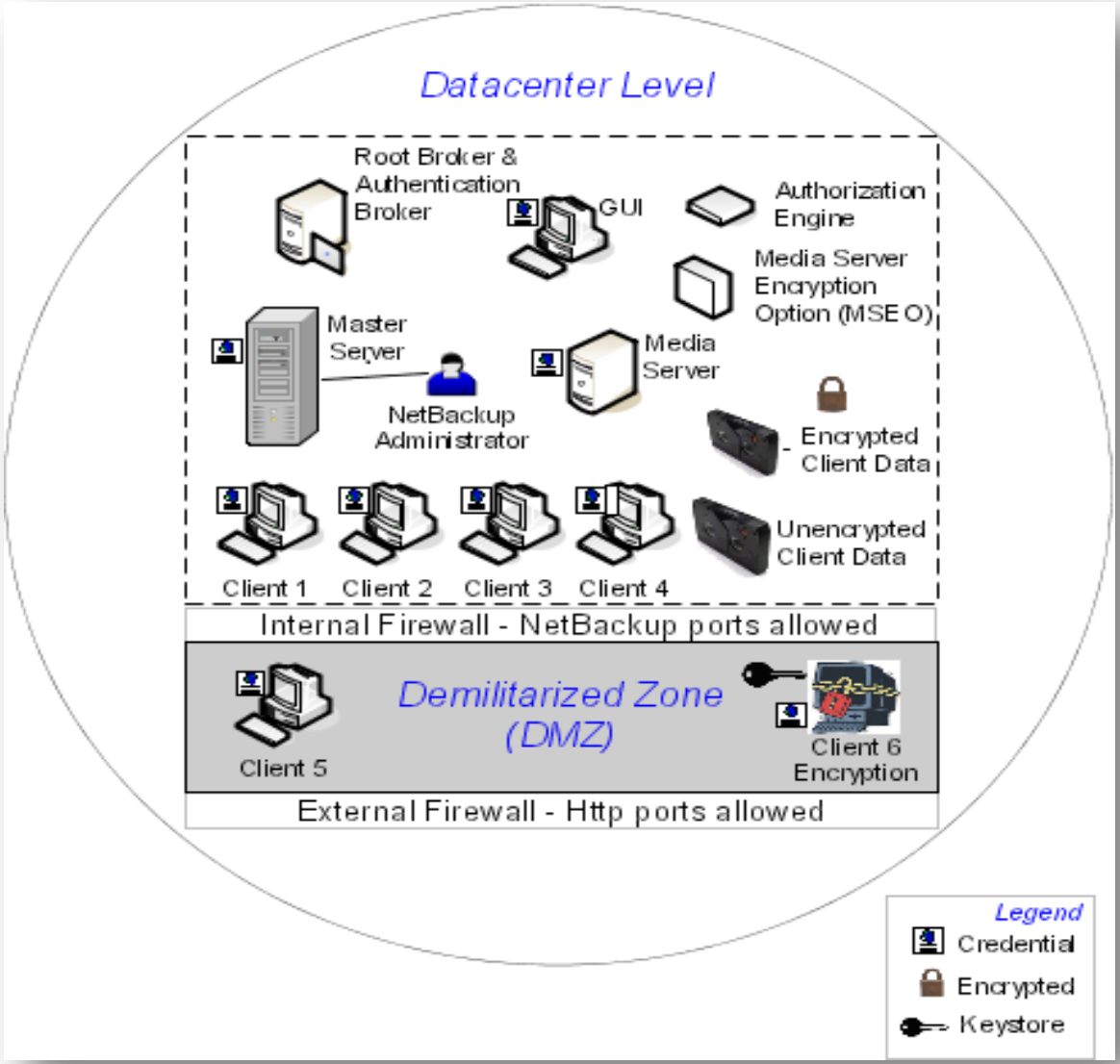
NBAC complete security-Example



- This combines all the security models together.
- The client requirements can necessitate using encryption off host
- Client requirements can also necessitate using encryption on host if the data on the host is sensitive.
- Incorporating NBAC allows segregation of administrators, operators, and users within NetBackup.
- For more information about All NetBackup Security, refer to the following article: http://www.symantec.com/docs/HOWTO46722

Whiteboards and Diagrams

- NBAC incorporates the NetBackup Product Authentication and Authorization into NetBackup. This increases security for the master servers, media servers, and clients.
- NBAC uses authentication identities from a trusted source to reliably identify involved parties.
- Access decisions can then be made for manipulation of NetBackup based on those identities.

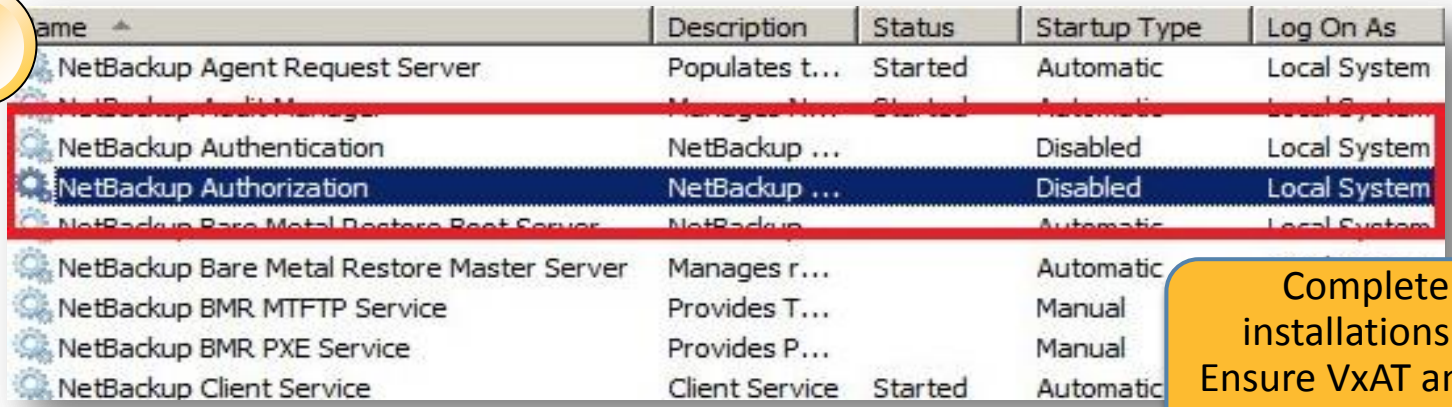


Notes on NBAC

- NBAC is now supported with Search.
- The command **`bpnbaz -setupindexserver`** helps support NBAC with search.
- Oracle, Oracle Archiver, DB2, Informix, Sybase, SQL Server, SAP, and EV Migrator are not supported with NBAC
- NBAC is not supported on Appliances
- For more information on NetBackup components that are used in security, refer the following article: http://www.symantec.com/docs/HOWTO46729

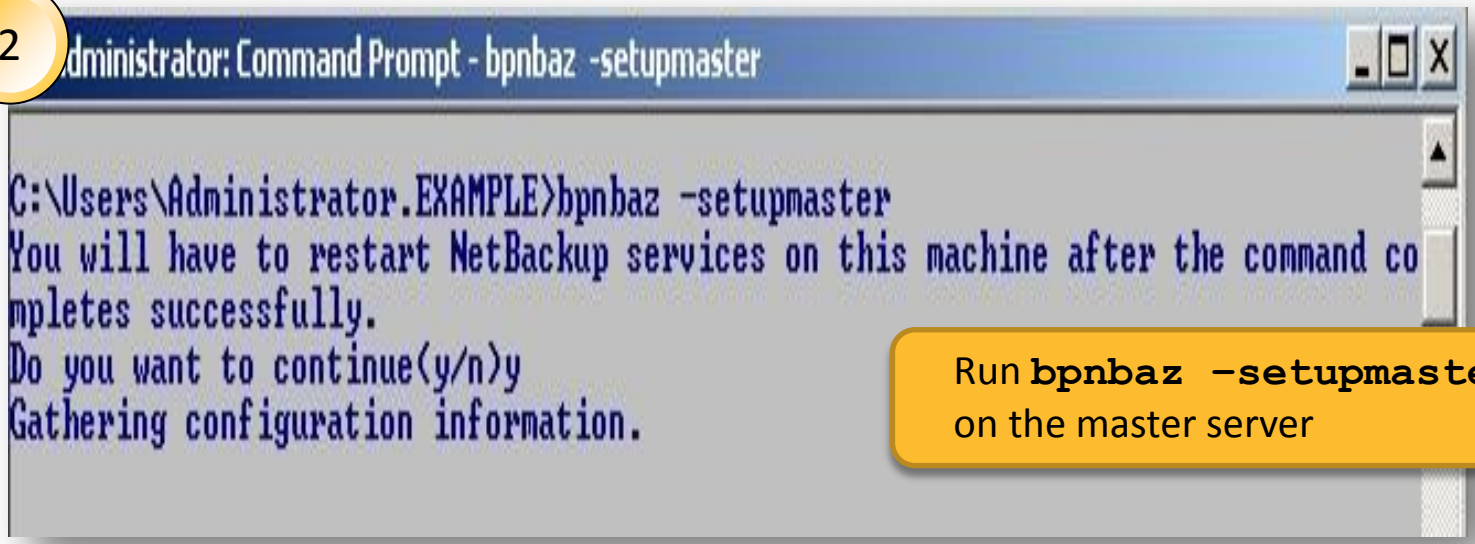
NetBackup Blueprints: Security
Configuring NBAC- Master server

1



Complete NetBackup installations and upgrade. Ensure VxAT and VxAZ services are not running

2



Run **`bpnbaz -setupmaster`** command on the master server

Configuring NBAC- Master server (1)

3

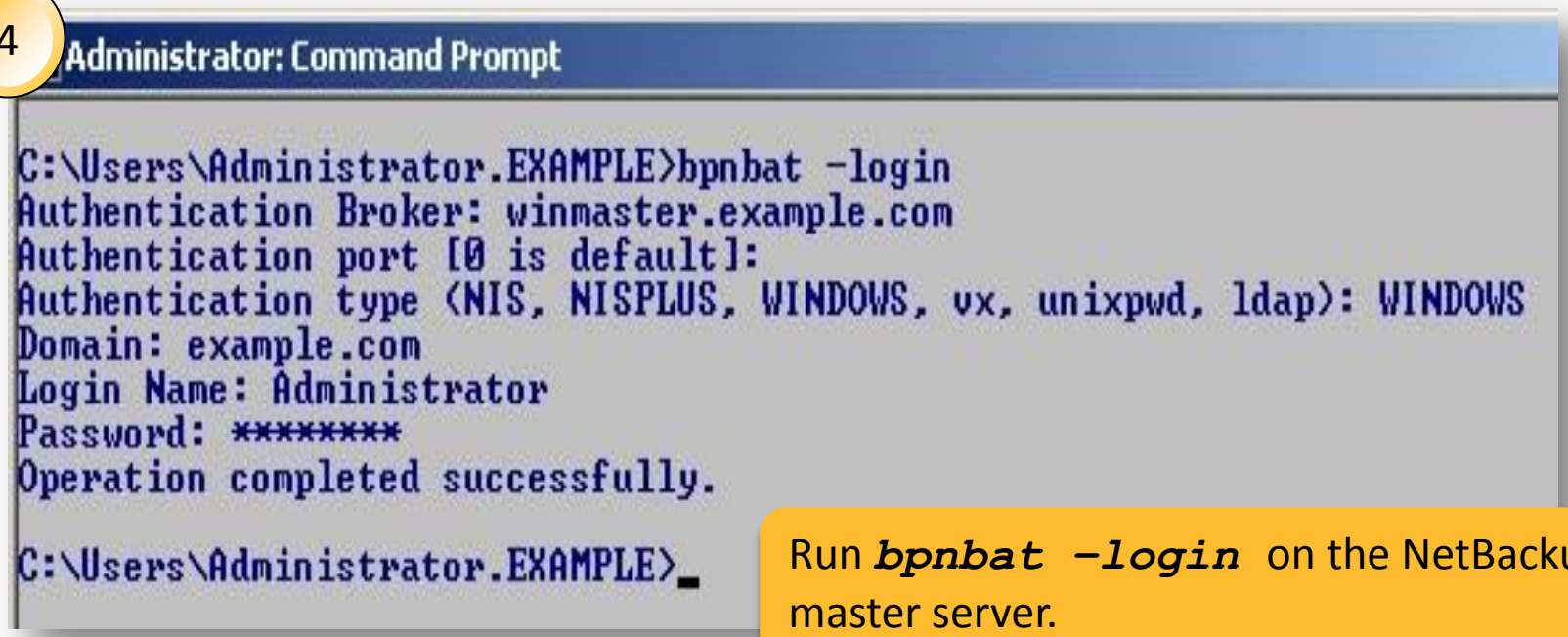
Name	Description	Status	Startup Type	Log On As
NetBackup Agent Request Server	Populates t...	Started	Automatic	Local System
NetBackup Audit Manager	Manages N...	Started	Automatic	Local System
NetBackup Authentication	NetBackup ...	Started	Automatic	Local System
NetBackup Authorization	NetBackup ...	Started	Automatic	Local System
NetBackup Bare Metal Restore Boot S...	NetBackup ...		Automatic	Local System

Restart the NetBackup services after the **`bpnbaz -setupmaster`** command completes successfully.

Following default users and groups are created after the services are started.

Configuring NBAC- Master server (2)

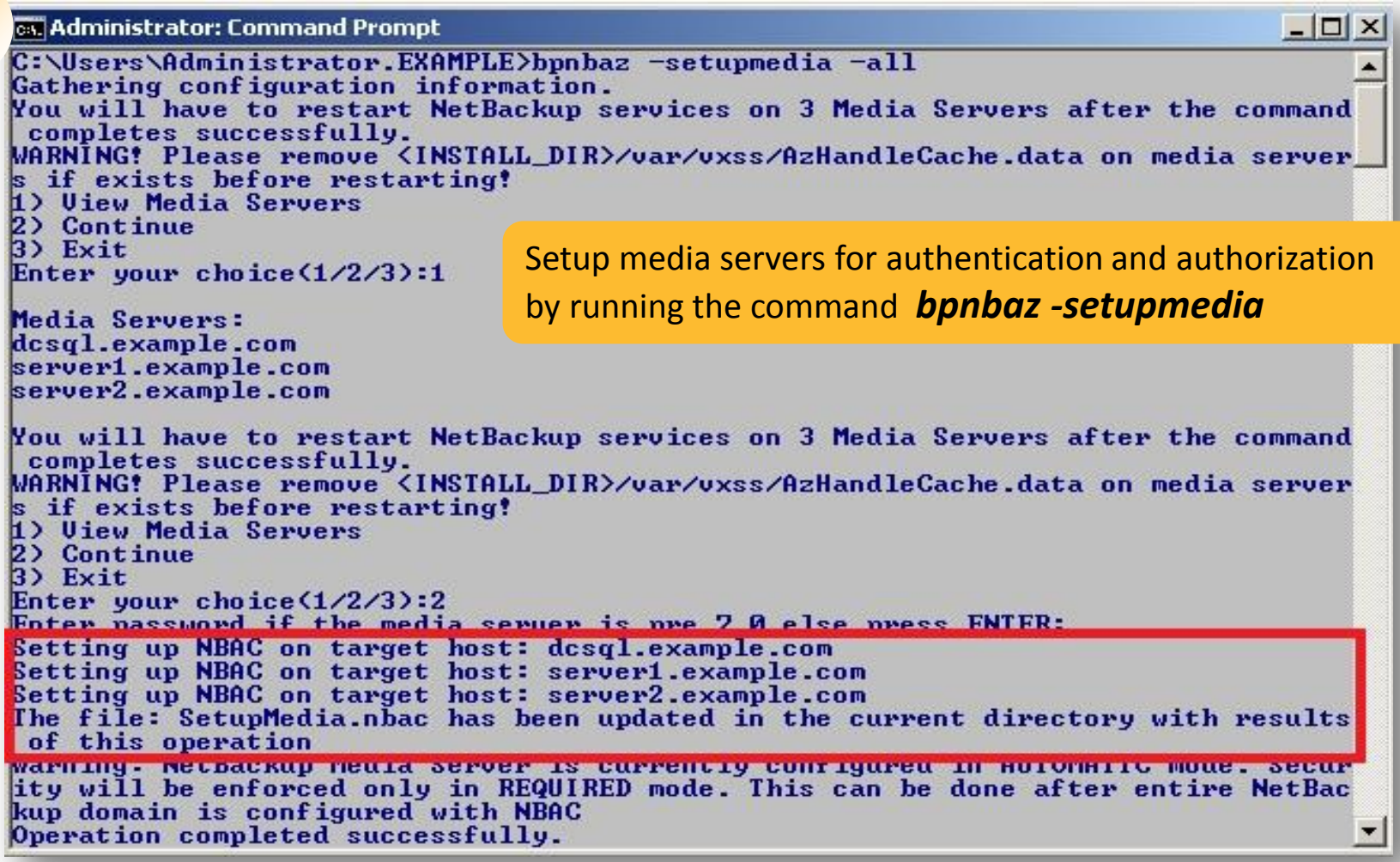
4



Run ***bpnbat -login*** on the NetBackup master server.

Configuring NBAC-Media Servers

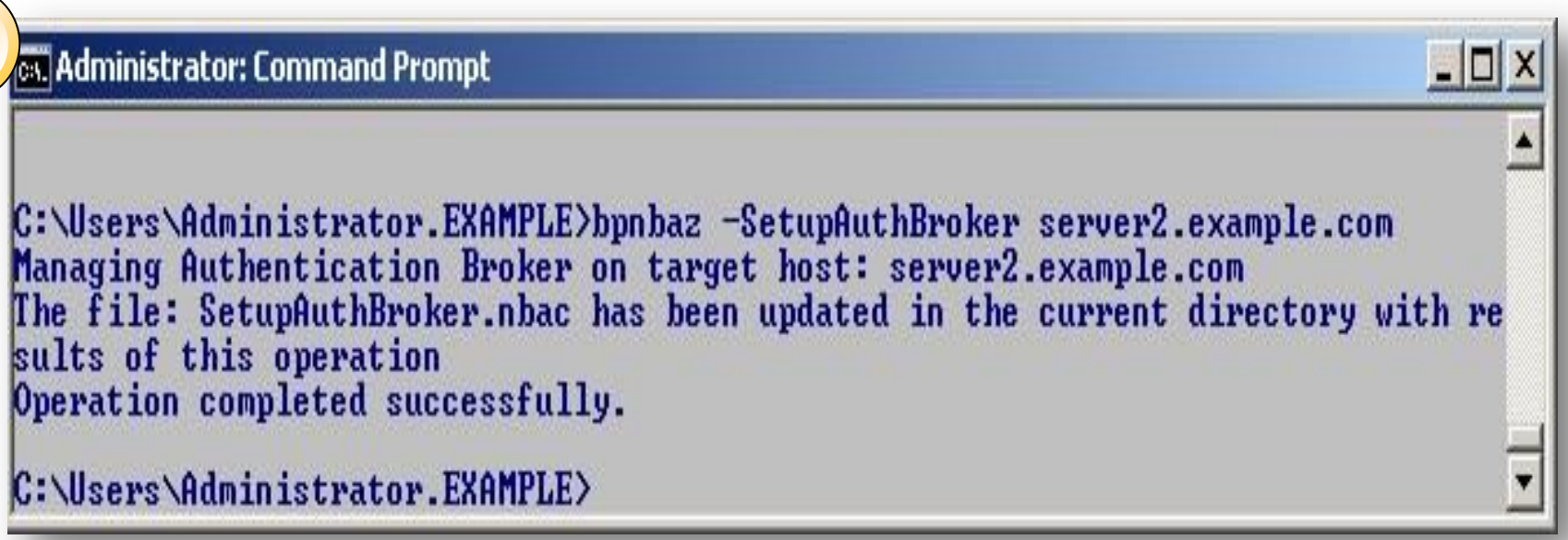
5



Setup media servers for authentication and authorization by running the command ***bpnbaz -setupmedia***

Configuring NBAC-Media Servers (1)

6



Setup a designated server as an authentication broker.

Run **`bpnbaz -SetupAuthBroker <server name>`** on the NetBackup master server.

Configuring NBAC-Media Servers (2)

7

```
C:\Users\Administrator.EXAMPLE>bpgetconfig USE_VXSS AUTHENTICATION_DOMAIN AUTHOR
IZATION_SERVICE > C:\temp\vxss_config.txt
```

Dump vxss configuration to a text file. This needs to be copied to remote UNIX media servers and Java admin console clients.

Navigate to `netbackup\bin\admincmd` location and run the following command:

```
bpgetconfig USE_VXSS AUTHENTICATION_DOMAIN
AUTENTICATION_SERVICE > C:\temp\vxss_config.txt
```

8

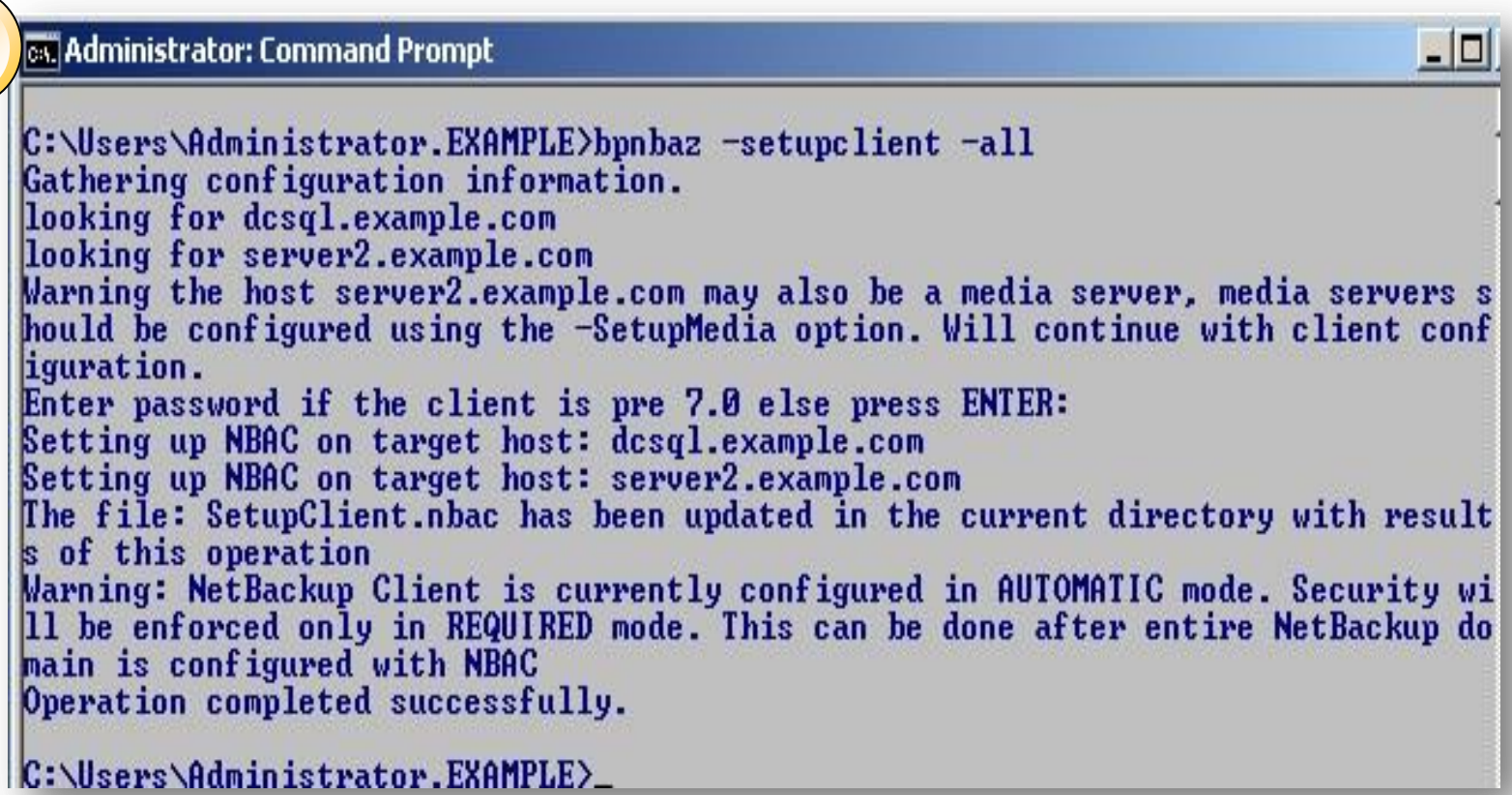
```
[root@server2 /]# bpsetconfig /tmp/vxss_config.txt
[root@server2 /]# more /usr/openv/netbackup/bp.conf
SERVER = winmaster.example.com
SERVER = server2.example.com
SERVER = server1.example.com
CLIENT_NAME = server2.example.com
USE_VXSS = AUTOMATIC
VXSS_SERVICE_TYPE = INTEGRITYANDCONFIDENTIALITY
EMMSERVER = winmaster.example.com
HOST_CACHE_TTL = 3600
VERBOSE = 0
AUTHENTICATION_DOMAIN = WINMASTER "ADDED AUTOMATICALLY" WINDOWS winmaster.exampl
e.com 0
AUTHENTICATION_DOMAIN = EXAMPLE "ADDED AUTOMATICALLY" WINDOWS winmaster.example.
com 0
AUTHENTICATION_DOMAIN = server2.example.com "ADDED AUTOMATICALLY" PASSWD server2
.example.com 0
AUTHORIZATION_SERVICE = winmaster.example.com 0
VXSS_NETWORK = server2.example.com AUTOMATIC
TELEMETRY_UPLOAD = NO
```

Copy NBAC setting generated on the master server to remote servers/clients:

`/usr/openv/netbackup/bin/admincmd/bpsetconfig /tmp/vxss_config.txt`

Configuring NBAC-Clients (1)

9

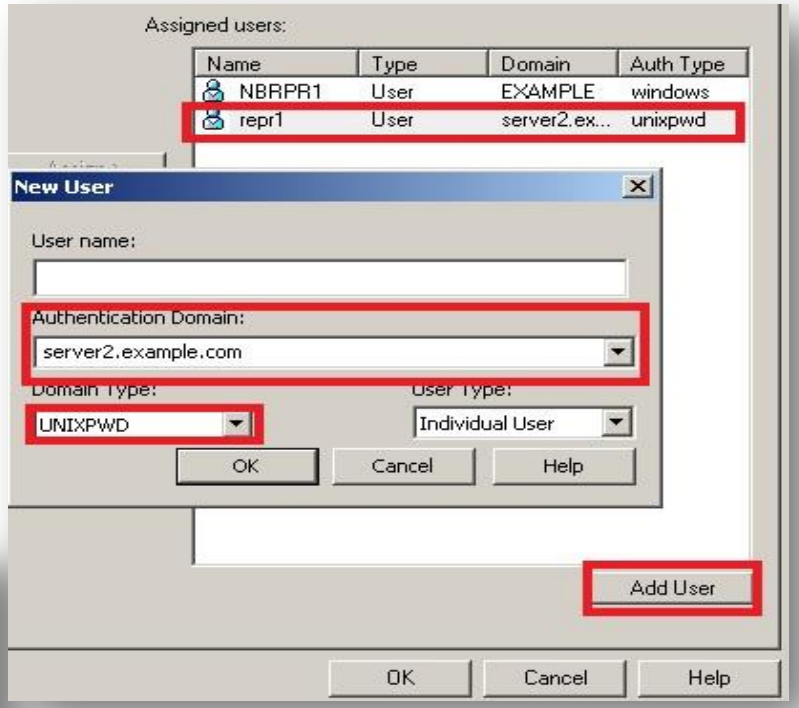


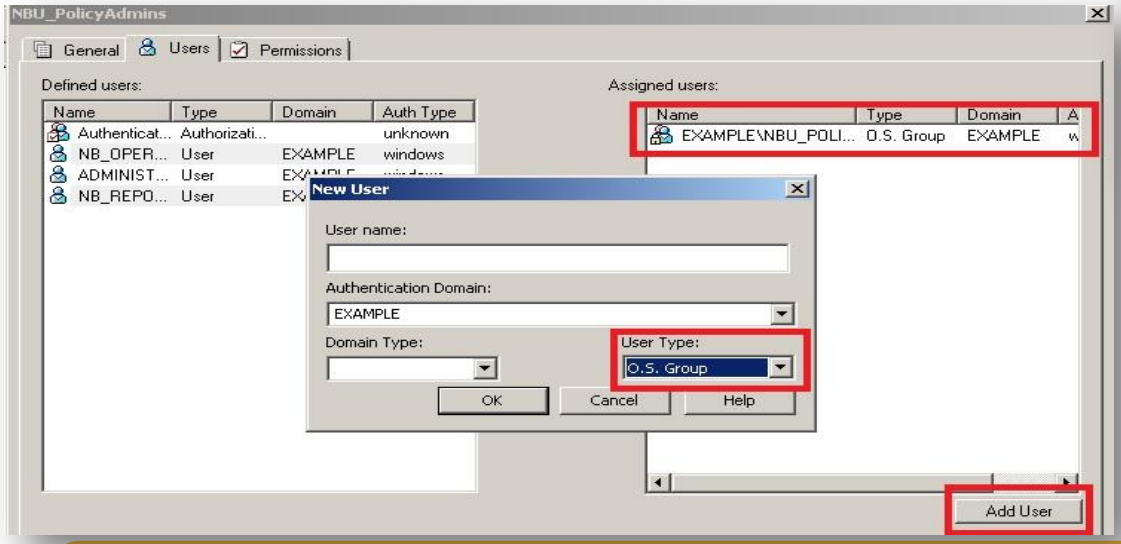
Setup Clients for the Authentication and Authorization

Configuring NBAC-Clients (2)

10

Add domain, workgroup users, and groups to the existing NetBackup authorization group. Custom NetBackup authorization groups can also be created as required. In this illustration, **NBU_Reporters** and **NBU_PolicyAdmins** are custom groups with customized permissions.





Frequently used NBAC Commands

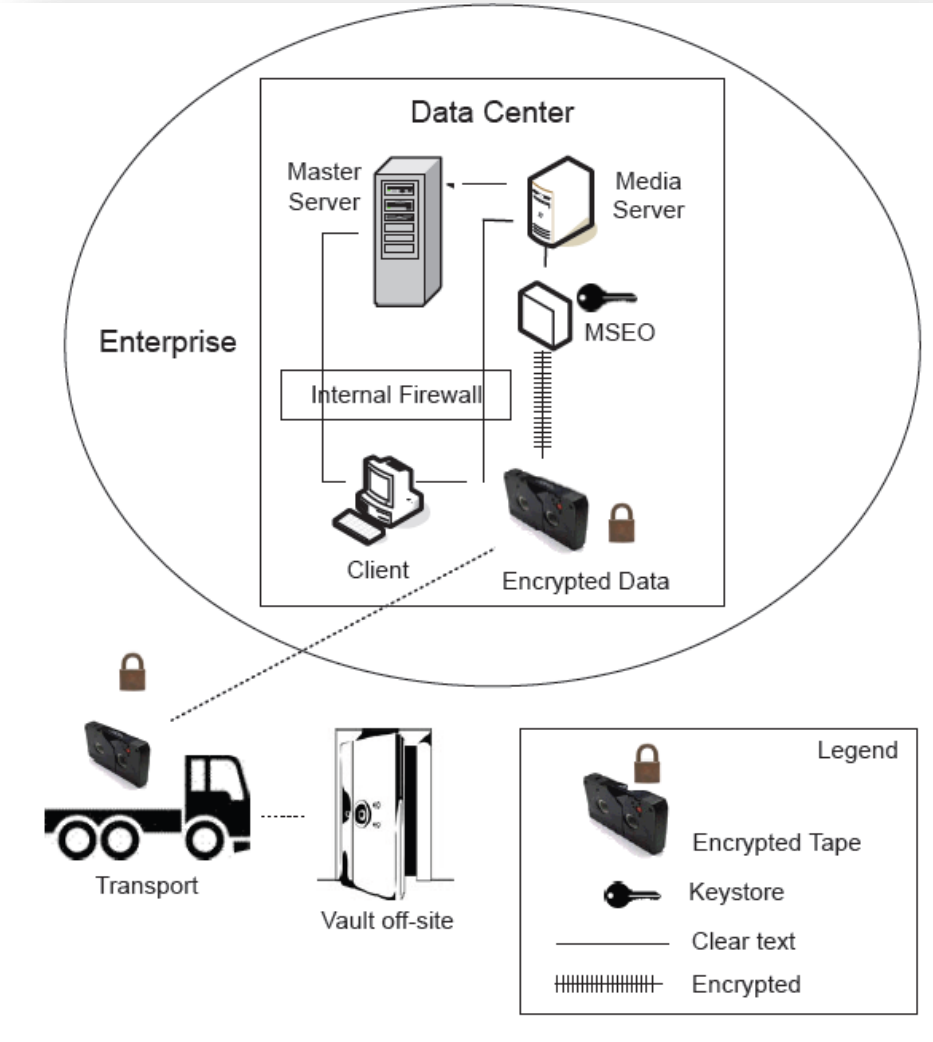
bpnbaz -SetupMaster	This command configures NBAC on the master server.
bpnbat -Login	This command can be used to update the credentials when it expires.
bpnbaz -SetupMedia	This command configures NBAC for the media servers.
bpnbaz -setupclient	This command configures NBAC for the clients.
bpnbaz -SetupAuthBroker	This command is used to setup Authentication Broker on a host.
bpnbat -whoami -cf	This command is used to verify master server, media server, or client settings for a particular host.
bpnbaz -GetConfiguredHosts	This command returns host names of all configured hosts. In a large environment, this could take some time to complete.
bpnbaz -ShowAuthorizers	This command helps verify, which computers can perform authorization lookups.
bpnbaz -listgroups	This command returns a list of authorization groups. This helps in verifying that the database is configured correctly.

Media Server Encryption Option (MSEO) Security

- Provides tape device drivers that fit between the NetBackup master server and the client media servers.
- Drivers are installed on each media sever in the NetBackup configuration.
- Read or write request to or from the storage medium, are intercepted by the MSEO virtual tape device and evaluated by a MSEO Security Server.
- Provides two graphical interfaces to configure MSEO Security Servers and their agents. One runs on the MSEO Security Server, and the other runs on each MSEO Agent.
- The MSEO interfaces are integrated with the NetBackup application

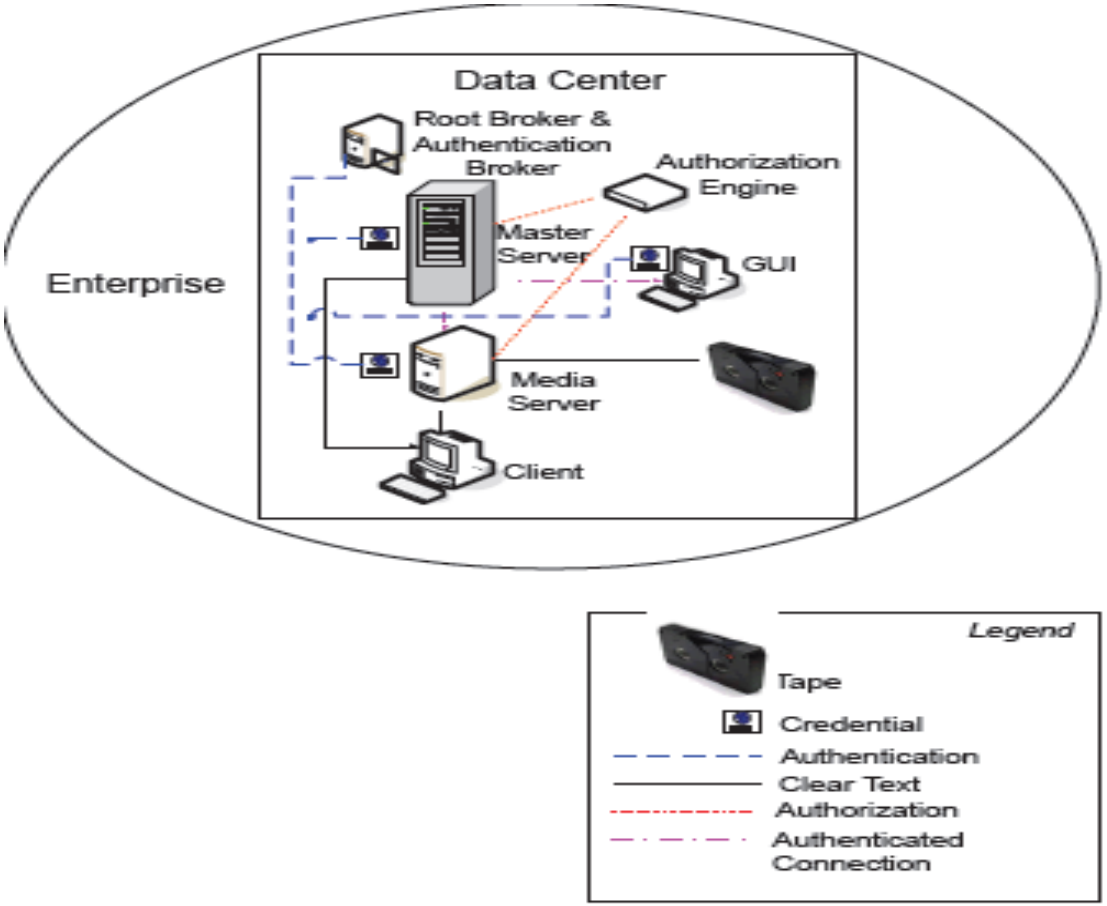
Media Server Encryption Option (MSEO) Security

- The MSEO Security Server keeps and manages the encryption keys necessary to read and write data.
- For more information about how to setup and configure MSEO, refer to the following article: http://www.symantec.com/docs/DOC7051



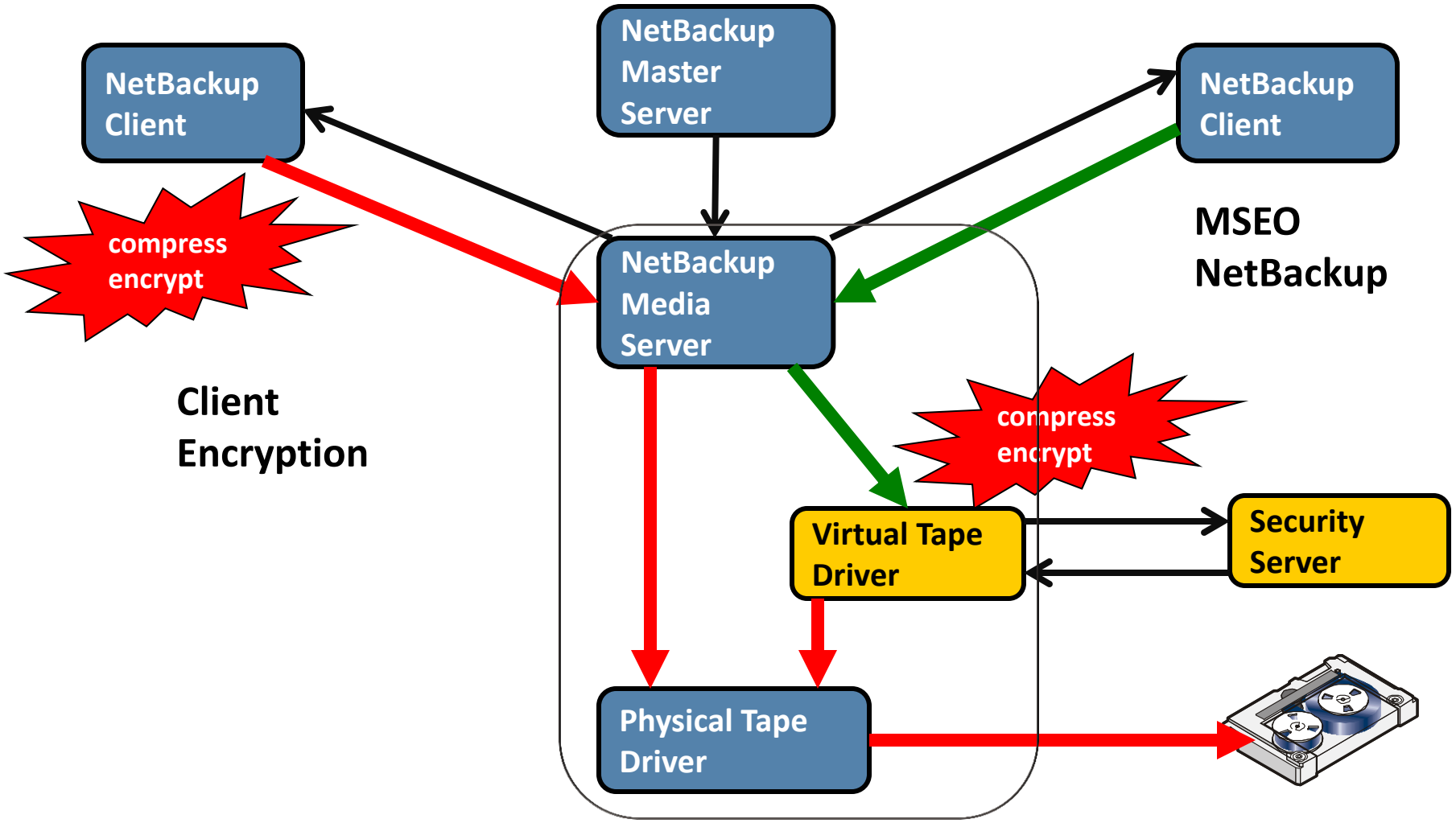
Client Side Encryption Security

- Ensures data confidentiality across the wire and on tape.
- Mitigates risk of passive wire tapping.
- Reduces risk of data exposure when tapes are moved offsite.
- The encryption key is located on the client.
- For more information , refer to the following article: http://www.symantec.com/docs/HOWTO46723

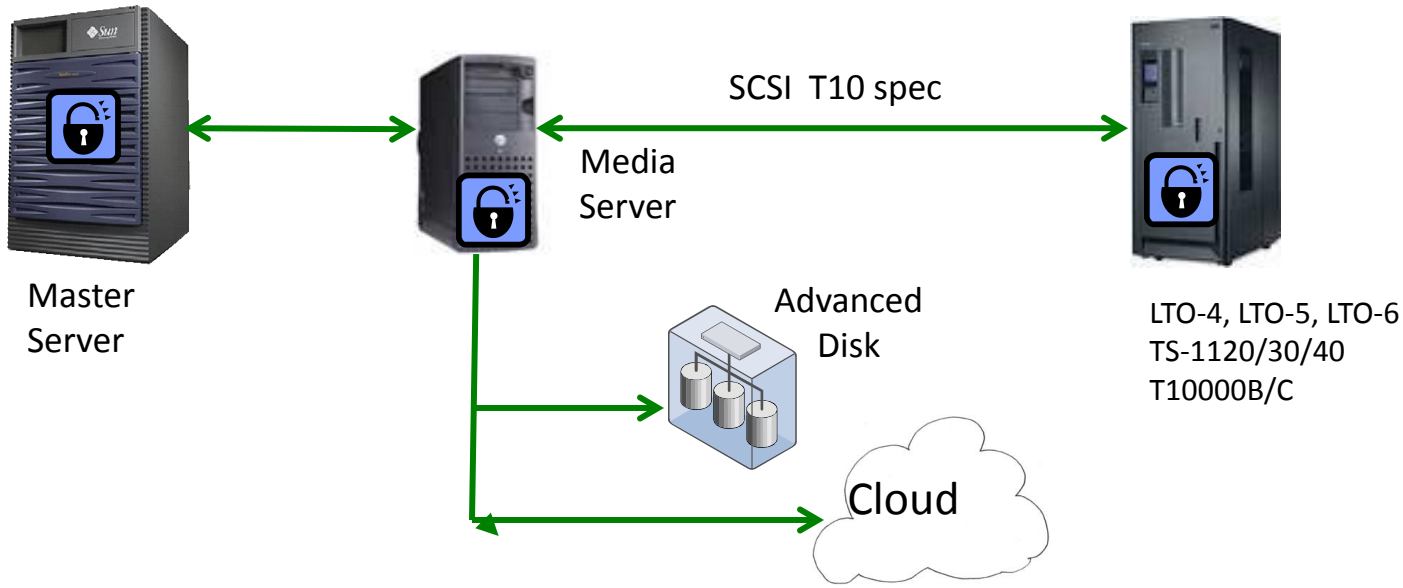


NetBackup Blueprints: Security

Difference between Client and Media Server Encryption

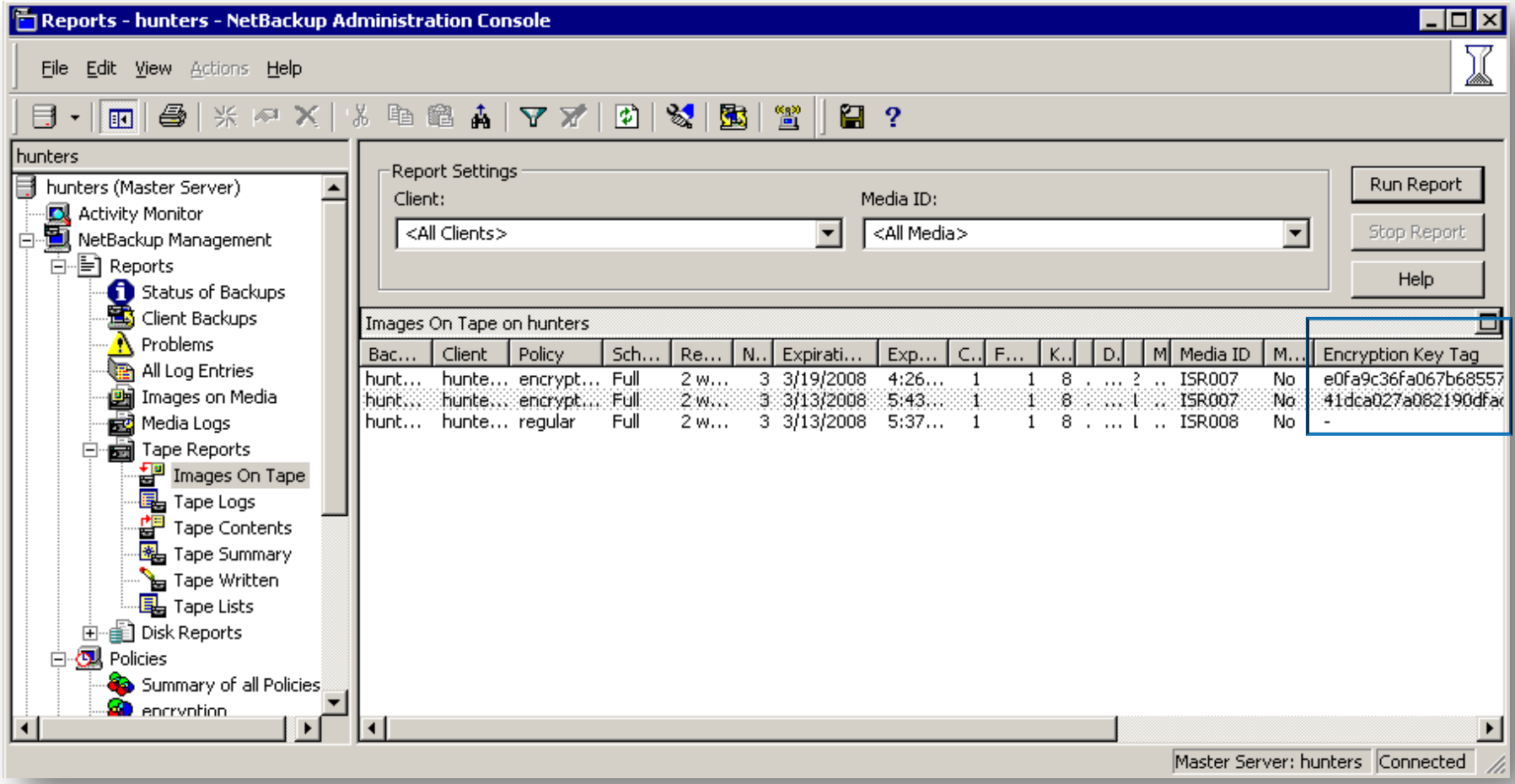


NetBackup Blueprints: Security
NetBackup Key Management Service (KMS)



- A symmetric Key Management Service. It is a part of the NetBackup Enterprise Server and NetBackup Server software.
- Runs on the NetBackup master server. No additional licenses are required to use the KMS functionality.
  For additional information, refer to the following article:
  http://www.symantec.com/docs/HOWTO71041

The **Encryption Key Tag** column in NetBackup Admin Console and reports (or via *bpimagelist* command) indicates which backup images are encrypted.



KMS data files

- Key Database

Located at `/opt/openv/kms/db/KMS_DATA.dat`

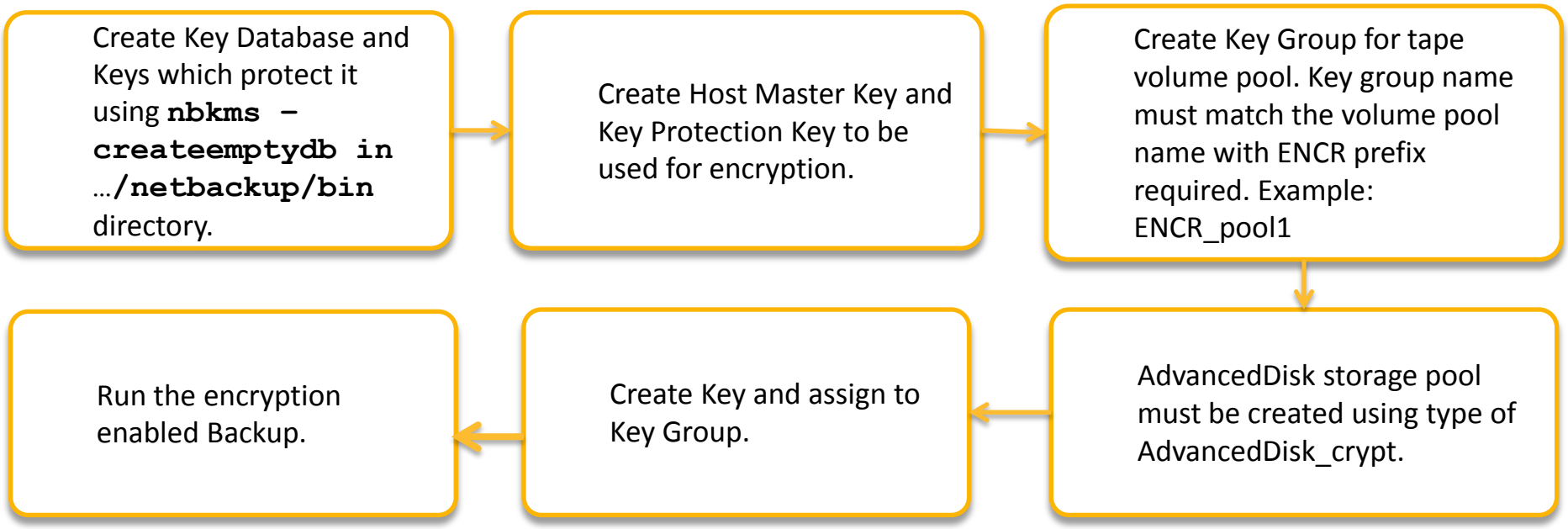
- Host Master Key

Encryption key protecting entire Key Database
Located at `/opt/openv/kms/key/KMS_HMKF.dat`

- Key Protection Key

Encryption key protecting data Encryption keys within the Key Database
Located at `/opt/openv/kms/key/KMS_KPKF.dat`

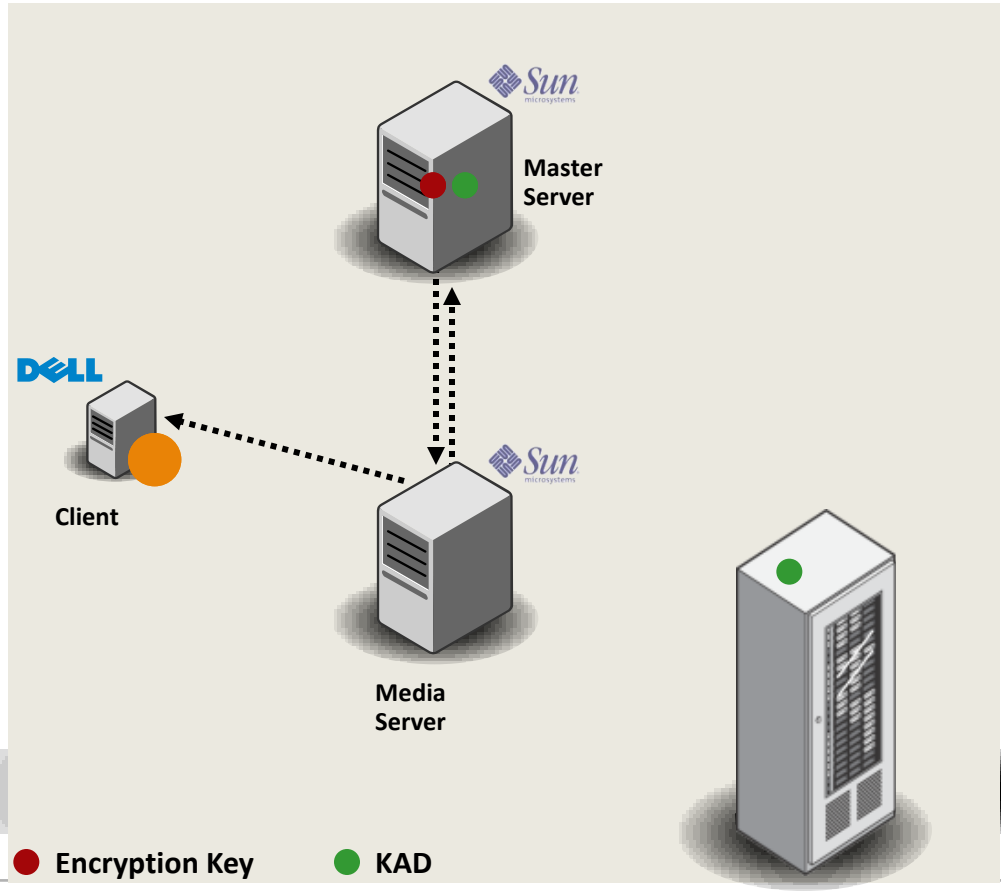
NetBackup Blueprints: Security
Steps to install and configure the KMS



For more information about Installing Key Management Service (KMS), refer to the following article: http://www.symantec.com/docs/HOWTO70193

For more information about installation and configuration of Key Management Service (KMS), click the following link: http://www.symantec.com/docs/TECH67972

Encryption: How it works?



1. Master starts backup.
2. Media server determines backup is to be encrypted and requests KAD (Key-Associated Data) and Key from Key Store.
3. Key Store provides active Key and KAD (Key-Associated Data) to media server.
4. Client provides data to media server.
5. Media server sends KAD (Key-Associated Data), Key, and backup image to tape drive.
6. Tape drive writes KAD (Key-Associated Data) on tape and encrypts backup image using Key.

NetBackup Blueprints: Security

How backup and restore works for Advanced disk and Cloud storage

Backup

- Master starts the backup.
- Media server determines backup is to be encrypted and requests Key Tag and Key from Key Store.
- Key Store provides active Key and Key Tag to media server.
- Client provides data to media server.
- Media server encrypts data using key and sends encrypted data, with Key Tag as attribute, to AdvDisk/Cloud storage.

Restore

- Restore requested from media server.
- Media server requests data from disk/cloud storage.
- Disk/cloud storage provides data, with Key Tag as attribute, to media server.
- Media server provides Key Tag to Key Store and requests Key.
- Key Store provides associated Key to media server.
- Media server decrypts data and sends data to client.

Encryption with Deduplication

- Encryption for Deduplication backup must be enabled via the **pd.conf** file on the host, which performs the deduplication process (client or media server).
- Deduplication encryption uses Blowfish 128-bit encryption algorithm.
- Protects data in transit and at rest.
- It do not require any separate key management as a separate key is generated for each unique segment internally
- Keys is sent with data and stored in both refDB and container files.

Best Practices

Choosing a NetBackup Security Solution

	Client Encryption	Media Server Encryption Option	KMS Managed Encryption	NetBackup Deduplication
Encryption Target	Existing tape drives or disk	Non-encrypted tape drive focus	Encrypted tape drives, Cloud, AdvancedDisk	Dedupe storage pool
Where Data is Encrypted	In transit and on tape and disk	In transit and on tape	On tape, in transit and on disk	In transit and on disk
Encryption	Software	Software	Hardware or software	Software
Key Store/Manager	On each client	Centralized across domain(s)	Centralized on master	N/A
OS Platform Support	All standard clients	Solaris, Windows, Linux	All major platforms	All major platforms
Software Cost	Free	Security Server and each media server	Free	Disk Protection Optimization Option

NetBackup Blueprints: Security
What gets stored where?

Location	Client Encryption	Media Server Encryption Option	KMS
Key store	Encryption Key (EK) Checksum of EK and cipher used	Public Key Private Key	Encryption Key Key Tag (KAD)
Stored on Tape	Checksum of EK and cipher used (in TAR header) Data encrypted by EK	EK encrypted with Public Key Hash of Public key Data encrypted by EK	KAD Data encrypted by EK
Stored on Disk	Checksum of EK and cipher used (in TAR header)	Not Applicable	Key Tag as Attribute Data encrypted by EK
Unique Encryption Key	Per client	Per backup job	Per tape volume pool or disk storage pool

	Key Management	Encryption
Client	Run bpkeyutil command to create key file and passphrase	Specify encryption attribute in policy (also enable compression for tape backups)
MSEO	Create key pairs and encryption policies	Configure MSEO tape drives on media servers
MSDP/Client Dedupe	None	Enable via pd.conf file on each host
KMS Tape	Create KMS db, key groups and keys using CLI	Create volume pool with ENCR suffix matching key group name
KMS Cloud	Use wizard to create KMS db and encryption key	Use wizard to create Storage Server and Storage Pool for encryption
KMS AdvancedDisk	Create KMS db, key groups and keys using CLI	Use nbdevconfig to create Storage Server and Pool for encryption

Encrypting data on Disk: Noteworthy points

	Client Encryption	Media Server Encryption Option	KMS and Tape Drive Encryption
Encryption Key	Per client	Per backup job	Per volume pool
Encryption policy basis	Per backup policy	Backup policy, client, media ID, copy #, volume pool, etc.	Per volume pool
Encryption (and compression) performed in	Software	Software	Hardware

Encrypting data on Disk: Noteworthy points

	Client Encryption	NetBackup Deduplication	NetBackup KMS
Encryption Key	Per client	Per segment	Per storage pool
Encryption policy basis	Per client	Per host (client or media server)	Per AdvancedDisk or Cloud storage pool
Encryption performed in	Software	Software	Software

- Backup the Key Database separately from Host Master Key (HMK) and Key Protection Key (KPK) files.
- If a tape with all three files is lost, all keys in Key Database are compromised.
- Do not encrypt the backups of these files. Equivalent of “locking the keys in the safe” and modern cryptography doesn’t allow “picking the lock”.
- Backup Key Database with your catalog backup.
- Host Master Key (HMK) and Key Protection Key (KPK) files do not change, so one backup will suffice. However, a periodic backup is recommended.
- By using pass-phrases to generate Host Master Key (HMK) and Key Protection Key (KPK) (and saving them), both key can be recreated to decrypt Key Database.

- NetBackup Security and Encryption Guide

http://www.symantec.com/docs/DOC6486

- NetBackup Cloud Administrator Guide

http://www.symantec.com/docs/DOC6458

- NetBackup AdvancedDisk Storage Solutions Guide

http://www.symantec.com/docs/DOC6463

- Symantec NetBackup Deduplication Guide

http://www.symantec.com/docs/DOC6466

- How to Export and Import Encryption Keys Using the NetBackup KMS

http://www.symantec.com/docs/TECH143390

Thank You!

Symantec Backup and Recovery Technical Services