Administration Manual for Infscape AWS UrBackup Appliance 1.0

Infscape UG (haftungsbeschränkt)

November 24, 2016

Contents

1 Introduction

Infscape AWS UrBackup Appliance is an advanced client/server backup system with clients for Windows, Linux and macOS, server to server replication and hybrid backup to cloud (AWS S3). Backups are deduplicated and compressed before being stored to S3, which leads to lower AWS S3 costs due to the decreased storage usage especially for long-term backup archival. The appliance does both image and file backups, allowing the appropriate selection of the preferred backup method depending on organization requirements and procedures. A wide range of applications such as databases are directly supported by the clients, making setting up backups easy.

2 Installation

2.1 Infscape AWS UrBackup Appliance installation

This section only gives a coarse overview over the required AWS configuration and setup. For more detailed instructions please see the AWS Quickstart Guide at `http://www.infscape.com/wp-content/uploads/2016/11/AwsUrBackupApp-Quickstart.pdf`.

2.1.1 Prerequisites

AWS S3 access Infscape AWS UrBackup Appliance stores all data into one Amazon S3 bucket. All other instance attached volumes are transient, i.e., it can recover from losing them, given the S3 encryption key is available. The appliances gets access to the S3 bucket via IAM role. It needs to be able to list the objects in the bucket and get its location.

Example IAM policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1460057323556",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketLocation"
            ],
            "Resource": "arn:aws:s3:::app-s3-test"
        },
        {
            "Sid": "Stmt1460057323557",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject"
            ],
            "Resource": "arn:aws:s3:::app-s3-test/*"
        }
    ]
}
```

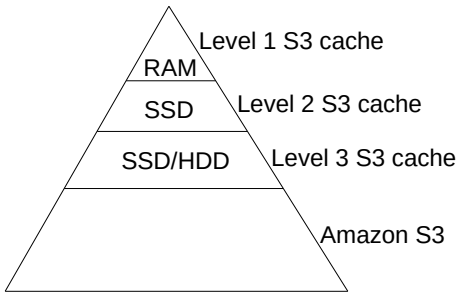

Figure 1: Appliance cache hierarchy illustration

EBS volume setup The first volume (automatically attached) contains the operating system, logs and databases. Because of the databases this volume should have SSD style IOPS. Choose at least "General Purpose SSD" as EBS volume type.

The second volume will be used as swap space. Swap space helps maximize the amount of RAM available. 4 GB of "General Purpose SSD" is enough.

The third volume will be used as level 2 S3 cache and all remaining volumes will be used as level 3 S3 cache. If the third volume is the last volume, it will be used as level 3 S3 cache and the appliance will have no level 2 S3 cache. Level 2 S3 cache should be faster (number of IOPS) than the level 3 s3 cache and can be smaller than the level 3 S3 cache (see figure 1). The larger the level 3 cache, the less active data must be stored and retrieved from S3 during a backup. The level 3 S3 cache is persistent, that is an appliance restart does not cause the appliance to retrieve previously cached items. If the level 3 S3 cache is put on non-persistent instance storage, more data has to be retrieved from S3 once the instance storage is cleared.

CPU requirements Backups are usually IO and not CPU limited. The appliance does however perform background and foreground compression of the level 3 S3 cache. Faster/more CPUs therefore can increase level 3 S3 cache efficiency and overall performance.

Account registration The backup appliance does not need a registered account to run. An account allows you to reset your appliance password via email in case the password is lost. The appliance encryption keys are automatically uploaded to your account (encrypted by the appliance admin password), such that you can more easily recover your appliance from S3 in case the first EBS volume is lost (this can be disabled). The appliance will allow account registration or selection during the appliance setup process.

Secure access during setup To securely access the appliance web interface either use AWS CloudFront serving HTTPS in front of the EC2 instance (using e.g elastic IP address ec2-11-11-11-11.eu-west-1.compute.amazonaws.com as origin) or put the instance into a private network which you can access via VPN.

If using CloudFront make sure to allow the POST method and set "Query String Forwarding" to "Forward all, cache based on all". The origin should be HTTP only and the front HTTPS only.

Security rules The appliance requires following ports to be forwarded (inbound):

Port	**Usage**	**Incoming/Outgoing**	**Protocol**
80	HTTP web interface	Incoming	TCP
55415	Clients and replication	Incoming	TCP

If you plan to access the appliance via SSH you should also allow SSH port 22 (inbound).

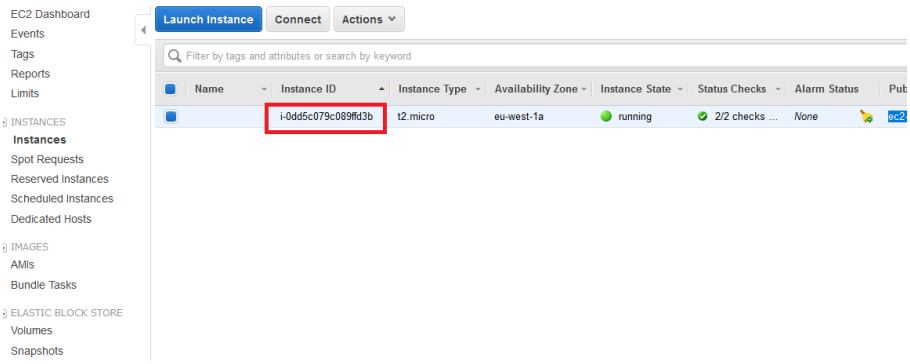

Figure 2: Instance id required during setup process

2.1.2 Initial appliance setup

Go to the the appliance web interface, e.g. `https://d3hh1iexxxxxx.cloudfront.net/` and enter the ec2 instance id to continue (see figure 2). Then follow the setup process.

2.2 Client installation

2.2.1 Windows/Mac OS X client installation

- Add a new Internet client on the status page.
- Download the client installer for the Internet client and send it to the new client. Alternatively, create a user for the new client (in the settings) and send the user the username/password. The user can then download the client installer from the server on the status page and install it.
- Select the backup paths you want to backup on the client or configure appropriate default directories to backup on the server (see section 6.3.4).
- The server will automatically start backups once the client is connected.

2.2.2 Automatic rollout to multiple Windows computers

First, if you want to deviate from the default backup path selection, configure the general default backup paths so that the correct folders get backed for each client (see section 6.3.4). Then install the clients using one of the following methods.

For internet clients:

Adapt the script at `https://urbackup.atlassian.net/wiki/display/US/Download+custom+client+installer+via+Python` to your server URL and create a python executable from the modified script via cx_Freeze (`http://cx-freeze.sourceforge.net/`). Executing the python executable on the client automatically creates a new internet client on the server, downloads a custom client and runs the installer. You could also add the silent install switch ("/S") when starting the downloaded installer such that it needs no user intervention.

2.2.3 Client installation on Linux

- Add a new Internet client on the status page.

- Download the client installer for the Internet client and send it to the new client. Alternatively, create a user for the new client (in the settings) and send the user the username/password. The user can then download the client installer from the server on the status page and install it.
- Select the backup paths you want to backup on the client via command line ("urbackupclientctl add-backupdir –path /" or configure appropriate default directories to backup on the server (see section 6.3.4).
- The server will automatically start backups once the client is connected.

3 Security

3.1 Server webinterface rights management

The server web interface is protected by a pretty standard user system. You can create, manage and delete accounts. Those accounts are only linked loosely to clients by rights management. An admin account can do everything including browsing file backups of all clients. The web interface allows one to create a limited account that can only browse backups and view statistics from one client. The more sophisticated rights editor can be used to allow an account to access several clients or to limit some aspects. For example you could setup an account which can do everything except browse backups. Following domains, with which you can limit or expand an account's rights, are currently available:

Domain	Description
browse_backups	Browse and download files from file backups
lastacts	View the last actions (file or image backups) the server did (including backup size and duration)
progress	View the progress of currently running file or image backups
settings	Allows settings to be changed
client_settings	Allows client specific settings to be changed
status	Allows the current status to be viewed (last seen, last file backup and last image backup)
logs	View the logs which were creating during backups
manual_archive	Manually archive file backups
stop_backup	Stop backups for client on the server
piegraph*	View statistics
users*	Get client names
general_settings*	Change general settings (like backup storage path)
mail_settings	Change the mail server settings
usermod*	Create, change and delete users
remove_client*	Remove clients and delete all their backups
start_backup*	Start backups for a client on the server
download_image	Download images of volumes from the server via restore CD

You can set the domains not marked with stars(*) either to one or several client ids (separated by ',') or to 'all' - meaning the account can access all clients. The entries with stars(*) have to be set to 'all' or 'none' and don't allow client ids. In order to be able to view statistics you need to set both 'piegraph' and 'users' to 'all'. There is a special domain 'all' which is a wild card for all domains (this means if you set 'all' to 'all' the account has the right to do everything).

Currently a user needs the "status" right for at least one client, in order for the user to be able to log in.

3.2 Client security

The client only processes commands if the server or the interface process supplies it with credentials. A random identity and private/public key pair.

The client interface credential is generated in the same way and resides in 'pw.txt' and 'pw_change.txt' in the installation directory on the client. To give the client core process interface commands you need the contents of 'pw.txt' or 'pw_change.txt' depending on what the command is:

pw.txt:

- Getting the current status
- Get the paths which are backed up during file backups
- Get the incremental file backup interval
- Start backups
- Pause backups

pw_change.txt

- Change the paths which are backed up during file backups
- Get all settings
- Change all settings
- Get log entries/logs
- Accept a new server

Per default only privileged users can access 'pw_change.txt'. On Windows this leads to a elevation prompt on selecting a menu item which requires the contents of 'pw_change.txt'. If you want to allow the commands without elevation prompt, either disable UAC or change the permissions on 'pw_change.txt' to allow non-privileged users read access. The client core process saves the server credentials from which it accepts commands and which it allows to download files in 'server_idents.txt' - one credential per line. The server's public key is also saved in 'server_idents.txt'.

If you want to manually add a server to 'server_idents.txt' you need to remove the preceding '#I' and '#' at the end of the contents of 'server_ident.key'. After installation the 'server_idents.txt' does not exist and the client core process accepts(and adds) the first server it sees (with the public key of the server). After that no other servers with different credentials are accepted and you need to add their credentials either manually, or via clicking on the popup box, once the client has detected the new server. This prevents others from accessing files you want to be backed up in public places.

If you want to have several servers to be able to do backups of a client you have two options. Either you manually supply the server credentials to the client (by copying them into 'server_idents.txt') or you give all servers the same credentials by copying the same 'server_ident.key', 'server_ident_ecdsa409k1.priv' and 'server_ident_ecdsa409k1.pub' to all servers.

3.3 Internet mode security

The Internet mode uses strong authentication and encryption. The three way handshake is done using a shared key, ECDH and PBKDF2-HMAC using SHA512 with 20000 iterations. The data is encrypted and authenticated using AES-GCM. Additionally the local network server authentication via server identity key and ECDSA private/public key authentication is done.

4 Backup process

4.1 Pre and post backup scripts on client and server

The client calls scripts previous and after backups on both the server and the client. This section will list the called scripts and the script parameters.

4.1.1 Client pre and post backup scripts

On Linux the clients pre and post backups scripts are searched for /etc/urbackup/ or /usr/local/etc/urbackup/ (depending on where urbackup is installed). On Windows they are searched for per default in C:\Program Files\UrBackup with a ".bat" file extension. All scripts except "prefilebackup.bat" on Windows have to be created first.

Script	Description	Parameters	On failure (return code not zero)
prefilebackup	Called before a file backup (before snapshot/shadowcopy creation).	1: "0" for full backup "1" for incremental file backup. 2: Server token. 3: File backup group	Indexing fails and backup is not started
postfilebackup	Called if a file backup successfully finished	No parameters	Ignored
preimagebackup	Called before a image backup (before snapshot/shadowcopy creation).	1: "0" for full backup "1" for incremental file backup. 2: Server token.	Image backup fails
postimagebackup	Called if a image backup successfully finished	No parameters	Ignored

4.1.2 Server post backup scripts

On Linux the post backup scripts are searched for in /var/urbackup or /usr/local/var/urbackup (depending on where urbackup is installed). On Windows they are searched for per default in C:\Program Files\UrBackupServer\urbackup with a ".bat" file extension. All scripts have to be created.

Script	Description	Parameters	On failure (return code not zero)
post_full_filebackup	Executed after a full file backup finished	1: Path to file backup. 2: “1” if successful, “0” otherwise. 3: File backup group	Backup fails
post_incr_filebackup	Executed after a incremental file backup finished	1: Path to file backup. 2: “1” if successful, “0” otherwise. 3: File backup group	Backup fails
post_full_imagebackup	Executed after a full image backup finished	1: Path to image backup file. 2: Image letter. 3: “1” if successful, “0” otherwise	Backup fails
post_incr_imagebackup	Executed after a incremental image backup finished	1: Path to image backup file. 2: Image letter. 3: “1” if successful, “0” otherwise	Backup fails

5 Server to server Replication

Infscape Urbackup Appliance can replicate file backups to other Infscape UrBackup Appliances. Replicating image backups is on the roadmap and will be implemented soon. Replication is supported passively and actively, that is you can replicate to an appliance even if it is byhind NAT or firewall and no ports are forwarded.

To connect two appliances you need to first add a replication port on one appliance and then add a replication destination on the other appliance with the same name. Replication uses the same port as configured in the settings in the “Internet” tab (default: 55415). The appliance where you add the replication destination will connect to the appliance where the replication port is configured.

As next step either of the appliances can be configured to replicate backups to the other appliance, either all backups or only backups of a certain client. You can also configure a window during which this replication should happen and limit the replication speed. The replication window sytax is identical to the usual window sytax (see section 6.3.1). Different speeds can be configured at different windows (see section 6.1.8).

6 Server settings

The UrBackup Server allows the administrator to change several settings. There are some global settings which only affect the server and some settings which affect the client and server. For those settings the administrator can set defaults or override the client’s settings.

6.1 Global Server Settings

The global server settings affect only the server and can be changed by any user with "general_settings" rights.

6.1.1 Server URL

URL to which the client will browse if a user selects “Access/restore backups”. For example “http://backups.company.com:55414/”. Default: “” (If empty “Access/restore backups” will not be available on the clients.)

6.1.2 Do not do image backups

If checked the server will not do image backups at all. Default: Not checked.

6.1.3 Do not do file backups

If checked the server does no file backups. Default: Not checked.

6.1.4 Autoupdate clients

If this is checked the server will send new versions automatically to its clients. The UrBackup client interface will ask the user to install the new client version. If you check silent autoupdate (see Section 6.1.4) it will update in the background. The installer is protected by a digital signature. Default: Checked.

6.1.5 Max number of simultaneous backups

This option limits the number of file and image backups the server will start simultaneously. You can decrease or increase this number to balance server load. A large number of simultaneous backups may increase the time needed for backups. The number of possible simultaneous backups is virtually unlimited. Default: 100.

6.1.6 Max number of recently active clients

This option limits the number of clients the server accepts. An active client is a client the server has seen in the last two month. If you have multiple servers in a network you can use this option to balance their load and storage usage. Default: 10000.

6.1.7 Cleanup time window

UrBackup will do its clean up during this time. This is when old backups and clients are deleted. You can specify the weekday and the hour as intervals. The syntax is the same as for the backup window. Thus please see section 6.3.1 for details on how to specify such time windows. The default value is 1-7/3-4 which means that the cleanup will be started on each day (1-Monday - 7-Sunday) between 3 am and 4 am.

6.1.8 Total max backup speed for local network

You can limit the total bandwidth usage of the server in the local network with this setting. All connections between server and client are then throttled to remain under the configured speed limit. This is useful if you do not want the backup server to saturate your local network.

All speed settings can have different values for different windows. See first how to specify a window at section 6.3.1.

You can set different speeds at different times by combining the speed setting with a window, separated by "@".

If you want a default speed limit of 60 MBit/s and 10 MBit/s during working hours (Mon-Fri, 8am to 6pm):

```
60;10@Mon-Fri/8-18
```

The most specific speed limit will be used, so adding an extra rule for 80 MBit/s for 12am to 1pm works as expected regardless of order:

```
60;10@Mon-Fri/8-18;80@1-7/12-13
```

6.2 Mail settings

6.2.1 Mail server settings

If you want the UrBackup server to send mail reports a mail server should be configured in the 'Mail' settings page. The specific settings and their description are:

Settings	Description	Example
Mail server name	Domain name or IP address of mail server	mail.example.com
Mail server port	Port of SMTP service. Most of the time 25 or 587	587
Mail server username	Username if SMTP server requires one	test@example.com
Mail server password	Password for user name if SMTP server requires credentials	password1
Sender E-Mail Address	E-Mail address UrBackup's mail reports will come from	urbackup@example.com
Send mails only with SSL/TLS	Only send mails if a secure connection to the mail server can be established (protects password)	
Check SSL/TLS certificate	Check if the server certificate is valid and only send mail if it is	
Server admin mail address	Address for fatal errors (such as if an emergency cleanup fails or other fatal errors occur)	

To test whether the entered settings work one can specify an email address to which UrBackup will then send a test mail.

6.2.2 Configure reports

To specify which activities with which errors should be sent via mail you have to go to the 'Logs' page. There on the bottom is a section called 'Reports'. There you can say to which email addresses reports should be sent(e.g. user1@example.com;user2@example.com) and if UrBackup should only send reports about backups that failed/succeeded and contained a log message of a certain level.
If you select the log level 'Info' and 'All' a report about every backup will be sent, because every backup causes at least one info level log message. If you select 'Warning' or 'Error' backups without incidents will not get sent to you.

Every web interface user can configure these values differently. UrBackup only sends reports of client backups to the user supplied address if the user has the 'logs' permission for the specific client. Thus if you want to send reports about one client to a specific email address you have to create a user for this client, login as that user and configure the reporting for that user. The user 'admin' can access logs of all clients and thus also gets reports about all clients.

6.3 Client specific settings

Settings	Description	Default value
Interval for incremental file backups	The server will start incremental file backups in such intervals.[1]	5h

[1] See section 6.3.2 for time specific intervals.

Interval for full file backups	The server will start full file backups in such intervals. [1]	30 days
Interval for incremental image backups	The server will start incremental image backups in such intervals. [1]	7 days
Interval for full image backups	The server will start full image backups in such intervals. [1]	30 days
Maximal number of incremental file backups	Maximal number of incremental file backups for this client. If the number of incremental file backups exceeds this number the server will start deleting old incremental file backups.	100
Minimal number of incremental file backups	Minimal number of incremental file backups for this client. If the server ran out of backup storage space the server can delete incremental file backups until this minimal number is reached. If deleting a backup would cause the number of incremental file backups to be lower than this number it aborts with an error message.	40
Maximal number of full file backups	Maximal number of full file backups for this client. If the number of full file backups exceeds this number the server will start deleting old full file backups.	10
Minimal number of full file backups	Minimal number of full file backups for this client. If the server ran out of backup storage space the server can delete full file backups until this minimal number is reached. If deleting a backup would cause the number of full file backups to be lower than this number it aborts with an error message.	2
Maximal number of incremental image backups	Maximal number of incremental image backups for this client. If the number of incremental image backups exceeds this number the server will start deleting old incremental image backups.	30
Minimal number of incremental image backups	Minimal number of incremental image backups for this client. If the server ran out of backup storage space the server can delete incremental image backups until this minimal number is reached. If deleting a backup would cause the number of incremental image backups to be lower than this number it aborts with an error message.	4
Maximal number of full image backups	Maximal number of full image backups for this client. If the number of full image backups exceeds this number the server will start deleting old full image backups.	5
Minimal number of full image backups	Minimal number of full image backups for this client. If the server ran out of backup storage space the server can delete full image backups until this minimal number is reached. If deleting a backup would cause the number of full image backups to be lower than this number it aborts with an error message.	2
Delay after system start up	The server will wait for this number of minutes after discovering a new client before starting any backup	0 min
Backup window	The server will only start backing up clients within this window. See section 6.3.1 for details.	1-7/0-24
Max backup speed for local network	The server will throttle the connections to the client to remain within this speed (see 6.1.8 for setting speed with window).	-

Perform auto-updates silently	If this is selected automatic updates will be performed on the client without asking the user	Checked
Soft client quota	During the nightly cleanup UrBackup will remove backups of this client if there are more backups than the minimal number of file/image backups until this quota is met. The quota can be in percent (e.g. 20%) or absolute (e.g. 1500G, 2000M).	""
Excluded files	Allows you to define which files should be excluded from backups. See section 6.3.3 for details	""
Default directories to backup	Default directories which are backed up. See section 6.3.4 for details	""
Volumes to backup	Specifies of which volumes an image backup is done. Separate different drive letters by a semicolon or comma. E.g. 'C;D'. Use the special setting "ALL" to backup all volumes and "ALL_NONUSB" to backup all volumes except those attached via USB.	C
Allow client-side changing of the directories to backup	Allow client(s) to change the directories of which a file backup is done	Checked
Allow client-side starting of incremental/full file backups	Allow the client(s) to start a file backup	Checked
Allow client-side starting of incremental/full image backups	Allow the client(s) to start an image backup	Checked
Allow client-side viewing of backup logs	Allow the client(s) to view the logs	Checked
Allow client-side pausing of backups	Allow the client(s) to pause backups	Checked
Allow client-side changing of settings	If this option is checked the clients can change their client specific settings via the client interface. If you do not check this the server settings always override the clients' settings.	Checked
Allow clients to quit the tray icon	Allow the client(s) to quit the tray icon. If the tray icon is quit current and future backups are paused.	Checked

6.3.1 Backup window

The server will only start backing up clients within the backup windows. The clients can always start backups on their own, even outside the backup windows. If a backup is started it runs till it is finished and does not stop if the backup process does not complete within the backup window. A few examples for the backup window:

1-7/0-24: Allow backups on every day of the week on every hour.
Mon-Sun/0-24: An equivalent notation of the above
Mon-Fri/8:00-9:00, 19:30-20:30;Sat,Sun/0-24: On weekdays backup between 8 and 9 and between 19:30 and 20:30. On Saturday and Sunday the whole time.

As one can see a number can denote a day of the week (1-Monday, 2-Tuesday, 3-Wednesday, 4-Thursday, 5-Friday, 6-Saturday, 7-Sunday). You can also use the abbreviations of the days

(Mon, Tues, Wed, Thurs, Fri, Sat, Sun). The times can either consist of only full hours or of hours with minutes. The hours are on the 24 hour clock. You can set multiple days and times per window definition, separated per ",". If specifying intervals with '-' the starting and ending day are included in the interval. You can also set multiple window definitions. Separate them with ";".

6.3.2 Advanced backup interval

Similar to the backup speed limit (see section 6.1.8) the backup intervals can be specified for different time intervals by combining them with a backup window (see previous section 6.3.1) separated by "@". The most specific backup interval will then be used.

For example, the default backup interval should be one hour and at night (8pm to 6am) it should be 4 hours:

```
1;4@1-7/20-6
```

If additionally the backup interval should be 6 hours during the week-end:

```
1;4@1-5/18-6;6@6,7/0-24
```

6.3.3 Excluded files

You can exclude files with wild card matching. For example if you want to exclude all MP3s and movie files enter something like this:

```
*.mp3;*.avi;*.mkv;*.mp4;*.mpg;*.mpeg
```

If you want to exclude a directory e.g. Temp you can do it like this:

```
*/Temp/*
```

You can also give the full local name

```
C:\Users\User\AppData\Local\Temp\*
```

or the name you gave the location e.g.

```
C_\Users\User\AppData\Local\Temp
```

Rules are separated by a semicolon (";")

6.3.4 Default directories to backup

Enter the different locations separated by a semicolon (";") e.g.

```
C:\Users;C:\Program Files
```

If you want to give the backup locations a different name you can add one with the pipe symbol ("|") e.g.:

```
C:\Users|User files;C:\Program Files|Programs
```

gives the "Users" directory the name "User files" and the "Program files" directory the name "Programs".

Those locations are only the default locations. Even if you check "Separate settings for this client" and disable "Allow client to change settings", once the client modified the paths, changes in this field are not used by the client any more.

Directory flags Each directory to backup has a set of flags. If you do not specify any flags the default flags will be used. Otherwise only the flags you specify are used.
Flags are specified by appending them after the backup location name (separated by "/"). Flags themselves are sparated by ",".

Flag	Description	Default
optional	Backup will not fail if the directory is unavailable	Not default
follow_symlinks	Symbolic links which point outside of the specified directory will be followed	Default
symlinks_optional	Backup will not fail if a symbolic link cannot be followed	Default
one_filesystem	Files outside of the first encountered file system will be ignored and not backed up	Not default
require_snapshot	Fail backup if no snapshot/shadow copy can be created of the location	Not default
share_hashes	Share file hashes between different virtual clients	Default
keep	Keep deleted files and directories during incremental backups	Not default

If you want to set the optional flag:

```
C:\Users|User files/follow_symlinks,symlinks_optional,share_hashes,optional
```

(The first three are default flags)

6.3.5 Virtual sub client names

Virtual sub clients allow you to have different file backup sets with one client. Once you specify virtual sub clients, multiple clients will appear with the name "clientname[subclientname]". You can change all file backup specific options for that client, such as default directories to backup, incremental file backup interval, max number of incremental file backups, ... The virtual sub client will always be online while the main client ("clientname") is online.

Separate the virtual sub client names via "|". E.g.

```
system-files|user-files
```

6.4 Internet settings

Settings	Description	Default value
Internet server name/IP	The IP or name the clients can reach the server at over the internet	""
Internet server port	The port the server will listen for new clients on	55415
Do image backups over internet	If checked the server will allow image backups for this client/the clients	Not checked
Do full file backups over internet	If checked the server will allow full file backups for this client/the clients	Not checked
Max backup speed for internet connection	The maximal backup speed for the Internet client. Setting this correctly can help avoid saturating the Internet connection of a client (see 6.1.8 for setting speed with window)	-
Total max backup speed for internet connection	The total accumulative backup speed for all Internet clients. This can help avoid saturating the server's Internet connection (see 6.1.8 for setting speed with window)	-
Encrypted transfer	If checked all data between server and clients is encrypted	Checked
Compressed transfer	If checked all data between server and clients is compressed	Checked
Calculate file-hashes on the client	If checked the client calculates hashes for each file before the backups (only hashes of changed files are calculated). The file then does not have to be transferred if another client already transferred the same file	Not checked
Connect to Internet backup server if connected to local backup server	If checked the client will connect to the configured Internet server, even if it is connect to a backup server on the local network.	Not checked

6.5 Advanced settings

In this section you will find global server settings which you only have to change for heavy or custom workloads. Most settings will need a server restart to come into effect.

6.6 Debugging: End-to-end verification of all file backups

This is a setting for debugging purposes or for the paranoid. If end-to-end verification is enabled UrBackup clients will create file hashes for every file for every file backup reading every file that is to be backed up. At the end of the backup process the hashes of the files stored on the server are compared to the hashes calculated on the client. If hashes differ the backup fails and an email is sent to the server admin.

6.7 Debugging: Verify file backups using client side hashes

At the end of file backups the server will go over all files in the backup and compare the file hashes with the client-side hashes.

6.8 Maximum number of simultaneous jobs per client

Maximum number of simultaneous jobs per client and all its virtual sub-clients. Increase this if you want it to e.g. simultaneously perform image and file backups.

7 Restoring backups

UrBackup protects whole machines from disaster by creating image backups and a users or servers files by creating file backups. Because the file backups size can usually be reduced by focusing on the most important data on a machine they can usually be run more often than the image backups. It makes sense to use image and file backups in tandem, backing up the whole machine less regularily than the important files via file backups.

7.1 Restoring image backups

Image backups can be restored with a Debian GNU/Linux based bootable CD/USB-stick. During image restore the machine to be restored must be reachable without network address tranlation from the server (or you forward the client ports in sections 8.1 to the restore client). While Linux supports many mainboards, disk controllers etc. you should always verify that the restore CD works on your specific hardware especially if you use exotic or new hardware. Drivers and firmware for some wireless devices and a program to configure is included but restoring via a wired network connection will be less trouble and faster and should be preferred. The restore itself is easy to use. After startup it will look for a backup server. If it does not find one, you can enter the backup server's IP/hostname and change your networking settings. After a backup server is found it will ask for a username and password. Use for example your admin account to access all clients and their image backups. Then you can select one image backup, select the disk you want to restore to and then it will restore. The target disk must be at least as large as the disk which was image backupped. Some hardware changes may cause Windows to bluescreen on startup after restore. If the startup repair fails, you may have to do a repair install using a Windows disk. You should test the different hardware combinations beforehand if you plan on restoring Windows to different hardware.

7.2 Restoring file backups

When performing file backups Infscape UrBackup Appliance creates a file system snapshot identical to the client's file system at that point in time. Those backups can be accessed via Windows file sharing (samba). The appliance automatically creates Windows file sharing users with identical passwords and access rights as the web interface users, so you can login as *admin* and access all backups and copy files in order to access or restore them.

You can also create a user for client(s), which allows the user to browse all backups of the client(s) via the Infscape UrBackup Appliance web interface and download individual files or whole directories as ZIP (limited to max. 4GB compressed size).

Users can directly access the web interface from the client if a server URL is configured. Either they right-click on the UrBackup tray icon and then click "Access/restore backups" which opens the browser, or they can right click a file/directory in a backup path and then click on "Access/restore backups" to access all backups of a file/directory.

When browsing backups the web interface will show a restore button if the client is online. The restore will ask for user confirmation. If the client includes a GUI component (tray icon), the user confirmation will popup for all active users on the client to be restored. If not acknowledged in time (timeout) or if declined the restore will fail. You can change this behaviour in *C:\Program files \UrBackup \args.txt* by changing "default" to "server-confirms" on Windows, or by changing the restore setting in */etc/default/urbackupclient* or */etc/sysconfig/urbackupclient* on Linux.

UrBackup is setup this way because a theoretical data loss scenario is an attacker taking control of your backup appliance, deleting all backups and then deleting all files on the clients via restores.

On Linux (and the other operating systems) you can also restore via command line from the client using *urbackupclientctl browse* and *urbackupclientctl restore-start*.

8 Miscellaneous

8.1 Used network ports

The Server binds to following default ports:

Port	Usage	Incoming/Outgoing	Protocol
80	HTTP web interface	Incoming	TCP
55415	Internet clients	Incoming	TCP
35623	UDP broadcasts for discovery	Outgoing	UDP

The Client binds to following default ports (all incoming):

Port	Usage	Protocol
35621	Sending files during file backups (file server)	TCP
35622	UDP broadcasts for discovery	UDP
35623	Commands and image backups	TCP

8.2 Nightly backup deletion

Infscape UrBackup Appliance automatically deletes old file and image backups during the cleanup time window. Backups are deleted when a client has more incremental/full file/image backups then the configured maximum number of incremental/full file/image backups. Backups are deleted until the number of backups is within these limits again.
If the administrator has turned automatic shut-down on, this clean up process is started on server start up instead (as the server is most likely off during the night). Deleting backups and the succeeding updating of statistics can have a huge impact on system performance.

During nightly backup deletion UrBackup also tries to enforce the global and client specific soft quotas. It is only able to delete backups if a client has already more backups than the configured minimal number of incremental/full file/image backups.

8.3 Emergency cleanup

If the server runs out of storage space during a backup it deletes backups until enough space is available again. Images are favoured over file backups and the oldest backups are deleted first. Backups are only deleted if there are at least the configured minimal number of incremental/full file/image backups other file/image backups in storage for the client owning the backup. If no such backup is found UrBackup cancels the current backup with a fatal error. Administrators should monitor storage space and add storage or configure the minimal number of incremental/full file/image backups to be lower if such an error occurs.

8.4 Archiving

UrBackup has the ability to automatically archive file backups. Archived file backups cannot be deleted by the nightly or emergency clean up – only when they are not archived any more. You can setup archival under Settings->Archival for all or specific clients. When an archival is due and the the server is currently in a archival window (See 8.4.1) the last file backup of the selected type will be archived for the selected amount of time. After that time it will be automatically not archived any more. You can see the archived backups in the "Backups" section. If a backup is archived for only a limited amount of time there will be a time symbol next to the check mark. Hovering over that time symbol will tell you how long that file backup will remain archived.

8.4.1 Archival window

The archival window allows you to archive backups at very specific times. The format is very similar to *crontab*. The fields are the same except that there are no minutes:

Field	Allowed values	Remark
Hour	0-23	
Day of month	1-31	
Month	1-12	No names allowed
Day of week	0-7	0 and 7 are Sunday

To archive a file backup on the first Friday of every month we would then set "Archive every" to something like 27 days. After entering the time we want the backups archived for we would then add

```
*;*;*;5
```

as window (hour;day of month;month;day of week). To archive a backup every Friday we would set "Archive every" to a value greater than one day but less than 7 days. This works because both conditions have to apply: The time since the last backup archival must be greater than "Archive every" and the server must be currently in the archive window.
Other examples are easier. To archive a backup on the first of every month the window would be

```
*;1;*;*
```

and "Archive every" something like 2-27 days.
One can add several values for every field by separating them via a comma such that

```
*;*;*;3,5
```

and "Archive every" one day would archive a backup on Wednesday and Friday. Other advanced features found in *crontab* are not present.