CLOUD INFRASTRUCTURE
MANAGED VIRTUAL SERVER (DEDICATED) USER GUIDE
WELCOME TO MANAGED VIRTUAL SERVER ON DEDICATED COMPUTE

For sales, account set-up enquiries and technical support, contact your Telstra representative or visit the Cloud Services website (www.cloud.telstra.com), where you’ll find all our contact details plus a glossary, FAQs and Our Customer Terms.

Note: we don’t provide assistance with issues specific to a customer’s local network, servers, operating systems and software (post-installation). Specialist technical support may be charged as an additional service.

CONVENTIONS USED IN THIS GUIDE

The following typographical conventions are used in this guide for simplicity and readability:

Web addresses, email addresses and hyperlinks are shown in bold italics, for example www.cloud.telstra.com.

Button names and titles/features on your computer screen are shown in italics.

User input is shown in typewriter font.
WHAT’S INSIDE

CHAPTER 1  OVERVIEW  5
CHAPTER 2  HOW IT WORKS  7
CHAPTER 3  DEDICATED RESOURCES – BLADES AND STORAGE  9
CHAPTER 4  YOUR MANAGED VIRTUAL SERVERS  17
CHAPTER 5  CREATE VIRTUAL SERVERS  18
CHAPTER 6  GROUP VIRTUAL SERVERS  23
CHAPTER 7  MODIFY OR DELETE A VIRTUAL SERVER  26
CHAPTER 8  SERVER ANTI-VIRUS PROTECTION  29
CHAPTER 9  BACKUPS  30
CHAPTER 10  VIRTUAL SERVER SNAPSHOTS  36
CHAPTER 11  SOFTWARE  38
CHAPTER 12  REPORTS  40
CHAPTER 13  APPENDIX A: INSTALL DATABASE BACKUP SOFTWARE (PLUG-INS)  47
CHAPTER 14  APPENDIX B: BACKUP AND RESTORE PROCEDURES FOR FILESYSTEM AND DATABASE SOFTWARE  74
CHAPTER 15  APPENDIX C: FIND A BACKUP SERVER NAME  107
CHAPTER 16  APPENDIX D: RESTORE A BACKUP FILE TO AN ALTERNATE SERVER  109
CHAPTER 1
OVERVIEW

There are three different types of virtual server available on Telstra’s cloud infrastructure. Each type offers different ways to create and manage your cloud resources.

This guide refers specifically to our managed virtual server on dedicated compute service and outlines your resources plus how to manage your virtual servers.

This service is available at data centres in Sydney, Melbourne and Perth.

Our cloud services allow you to use different server types in any combination. You can learn about our other types of virtual server services in the:

- **Virtual Server (Dedicated) User Guide**
- **Virtual Server (Shared) User Guide**

These user guides do not include detailed information about account management, networks and security, infrastructure design and pricing. This along with other information features in the following guides, which can be used in conjunction with this one:

- **Account Management Guide**
- **Network and Security User Guide**
- **Infrastructure Design Guide**
- **Pricing Guide – Australia**
- **Responsibilities Guide**

  You can also view the terms and conditions associated with your cloud service in *Our Customer Terms.*
CHAPTER 2
HOW IT WORKS

When you purchase this service, you complete an order form detailing the resources you need for us to set up your service. You also receive welcome emails, which include, on separate emails, the username and password (encrypted in the email) you need to complete the installation.

PHYSICAL ENVIRONMENT

On our managed virtual server (dedicated) service, physical blades are allocated entirely to your environment.

Your service includes a minimum of two blade (physical) servers that are physically separate from those of other data centre tenants. The processing capacity of each blade is also dedicated to you. Blades can be added or removed on request.

We manage the physical server environment according to defined service level agreements.

Our data centres house the physical resources used to provide your virtual servers and feature high availability and 24/7 security. For more details on our data centres, see the Network and Security User Guide.

NETWORK SETTINGS

When setting up this service, your virtual servers can be connected to either your public network (internet) or a private network. After a virtual server has been created, it can also be dual homed — that is, connected to both a public and private network. All virtual servers also have a management connection (interface) to the cloud for backups, alarming and other required cloud management activities.

You can modify access to your servers at any time. For full details, refer to the Network and Security User Guide.

AVAILABILITY

This platform is designed for high availability, providing redundancy, ensuring no single point-of-failure, and featuring performance monitoring and alarming. Part A of the Cloud Services section of Our Customer Terms sets out the availability of virtual servers and the cloud platform.

VMware® High Availability (VMHA) protects all virtual server hardware and software. Virtual servers can be automatically:

- Restarted on another physical blade if the physical blade it’s running on fails
- Reset if the operating system crashes

For more details, refer to the Network and Security User Guide.

THE CLOUD SERVICES MANAGEMENT CONSOLE

You can manage, configure and view elements of this service using our secure online Cloud Services management console at cloud.telstra.com/manage. Instructions on how to use the Cloud Services management console form most of the content in this guide.

There are many functions you can perform in the Cloud Services management console, including:

- View and submit requests to modify your dedicated resources (blades, clusters and active/performance storage)
- Request virtual servers that draw on your dedicated resources
• Configure your virtual servers and network
• View details of your virtual servers
• Request a backup configuration (including applications)
• Request virtual server snapshots
• View your virtual server’s performance details, server status, usage, thresholds and notifications, and activity log

For details about how to access the Cloud Services management console, see our Account Management Guide.

MANAGED VIRTUAL SERVER (DEDICATED) SERVICE
A managed virtual server (dedicated) service allows you to:
• Submit requests to create virtual servers
• Submit requests for us to add and configure individual virtual server resources

Our services come in a range of sizes, including varying amounts of cloud resources. Contact us to find out more about our different plans.

Learn more about managing cloud services in the Account Management Guide.

NETWORK RESOURCES
Network and security resources for your managed virtual servers (dedicated) can be created and managed in the Cloud Services management console, but are not detailed in this guide. Refer to the Network and Security Guide for information about:

• Virtual data centres
• Networks and network connections
• Firewalls
• Load balancers
• IPSec VPN
• SSL VPN
• VLAN Extension
• SMTP mail relay (optional service)
• Security (including denial of service and web content security)
• Security add-ons

Your use of network resources is calculated under your virtual data centre subscription.
CHAPTER 3
DEDICATED RESOURCES – BLADES AND STORAGE

VIEW DEDICATED RESOURCES

View your dedicated resources at any time via our secure online Cloud Services management console at cloud.telstra.com/manage.

The Dedicated Resources screen highlights the details of your blades, cluster(s) and active/performance storage (compared to active storage, performance storage offers higher performance and comes at a higher fee). You can request as much of each type of storage as you need in your cluster.

Any changes you make to your dedicated resources appear on this screen. You can also filter your view by blade type, cluster and virtual data centre location.

If you’re viewing this console screen for the first time after purchasing managed virtual server (dedicated), you’ll see the cluster you created, including a minimum two blades plus their CPU, RAM, storage type and capacity.

You can also check on the status of a blade – it may be awaiting activation or removal. And you can add blades and storage from this page.
1. Select a specific blade to reveal a summary of its details, including: the blade ID; the data centre it’s associated with; CPU; RAM; and the term of your service.

2. Select a storage type to reveal which virtual server(s) it’s allocated to, the amount of storage allocated plus storage removal options.

**WHAT IS A CLUSTER?**

A cluster is a grouping of the blades and storage you need to run your virtual servers. Virtual servers are then associated with a cluster.

Clusters provide a way to manage groups of blades and storage. Networks can connect between clusters. You might want to use resource pools to manage your CPU and RAM resources to separate, for example, your testing and development servers from your production virtual servers.

You can have different datastores in a cluster (e.g. for testing/development and production virtual servers). Each cluster:

- Contains at least two blades plus associated storage (each blade in your service can only be associated with one cluster)
- Must have blades of the same physical CPU and RAM to ensure high availability resilience
- Is visible to public and private network containers
- Can only be associated with one virtual data centre (i.e. a single network)
• Has its own physical RAM and CPU load, independent of other clusters
• Exists on a separate VLAN (you can have multiple VLANs on a blade)
• Has a name defined by you plus a cluster ID name defined by us

Limitations

• You can’t have a mix of virtual server types in the same cluster (e.g. self-managed virtual servers with managed virtual servers).
• There is a limit on the number of virtual servers we can deploy to a cluster for you. This is based on capacity limits in our infrastructure, including total amounts of CPU, RAM and storage.

Ensuring high availability in a cluster

• The service levels are dependent on enough high-availability capacity being maintained for each virtual server in a cluster. You must ensure enough RAM and CPU capacity is available to failover any virtual server within the cluster.
• When configuring a cluster for your policy, choose a percentage for CPU and RAM that reflects the number of blade failures you wish to support. For example, if you want to set aside capacity for two blade failures and there are 10 blades of equal capacity in the cluster, then specify 20 percent (2/10). For more information on capacity requirements, see VMware® vSphere’s high availability deployment best practices.
Cluster scenario

The following is an example of a customer with three types of clusters: the first two in this configuration have managed virtual servers (dedicated) and a third cluster contains virtual servers (dedicated).

1. Clusters 1 and 2 belong to this service: managed virtual server (dedicated)
2. Cluster 3 is part of the virtual server (dedicated) service (separate service)

BLADES (PHYSICAL SERVERS)

Your service includes a minimum of two blade (physical) servers that are physically separate from those of other data centre tenants. The processing capacity of each blade is also dedicated to your use. Blades can be added or removed on request. We manage the physical server environment according to defined service level agreements.

A blade chassis may be shared by multiple customers, but you will have your own dedicated blade server (i.e. the blades are unique) on the chassis.

Blades are available in the following configurations:

<table>
<thead>
<tr>
<th></th>
<th>2</th>
<th>2</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RAM</td>
<td>128</td>
<td>256</td>
<td>512</td>
</tr>
</tbody>
</table>

ADD A BLADE(S)

From Dedicated Resources, choose Add Blade/Storage and select Blade from the dropdown.
You'll be taken to the Request Blade Server form. Complete the requirements on the form in order to submit a request to us to add a blade(s) to your service.

**CONFIGURE BLADES**

You’ll need to decide:

- Which virtual server configuration to add the blade to (if you have more than one)
- The number of blades you’d like to add, up to a maximum of 10
- The amount of CPU per blade (2 or 4). If you order multiple blades of differing CPU, you’ll need to complete the Request Blade Server form for each different configuration
- The amount of RAM per blade (128GB, 256GB or 512GB)
- The length of time you want the blade(s) for. You can select 1/12/24/36 months as your minimum term

**Note:** each blade is allocated 1,000GB (1TB) of active storage by default, though the entire 1TB is not available after formatting. We give your blade an ID.

**CONFIGURE CLUSTERS**

Each blade you request to add must be allocated to a new or existing cluster. By default, a new cluster has a minimum of two blades allocated.

**REVIEW AND PURCHASE**

You can review your blades and cluster configuration, view the estimated fee and make changes to your request before submitting it to us.
REMOVE A BLADE

You must contact us to remove a blade(s) ensuring any virtual servers using resources on the blade won’t be affected by its removal. We need to manage your cluster so that if the blade with the highest specifications is taken out (in the case of fault or assurance/operation activities) that the remaining blades in the cluster can manage your virtual servers.

We may refuse a request to remove a blade if we determine its removal will affect high availability and the service levels.

Once your request is confirmed, the blade’s details will display with Removal in progress.

Notes:

- At least two blades must remain in a cluster at all times
- You’re responsible for removing all virtual servers from a blade before it’s removed
- You need to ensure that if a blade is taken out (in the case of fault or assurance/operation activities) that the remaining blades in the cluster can manage your virtual servers
- If you submit a request to remove a blade before the end of your selected minimum term, an early termination fee applies. See Part A of the Cloud Services section of Our Customer Terms for more information regarding early termination fees.
VIEW STORAGE

The Dedicated Resources page summarises the amount of Active storage and/or Performance storage allocated to your selected cluster.

Active storage is suitable for standard intense file, print and mixed workloads, offering up to 3,000 IOPS (input/output operations per second). Performance storage is our premium offering and comes at a higher fee. It is designed to meet demanding workloads of up to 10,000 IOPS, such as databases and business analytics.

You can have as much of each type of storage as required in a cluster.

MODIFY STORAGE

When you submit a request to us to add storage (datastores), it increases the capacity of your infrastructure. You can also submit a request to downsize the storage assigned to a cluster, though you need to ensure any virtual servers using the resources on that datastore aren’t affected.

Add storage

1. From the Dedicated Resources page, choose Add Blade/Storage and select Storage from the dropdown. This takes you to the Request storage page.
Or you can access the Request storage page from the Active storage details page. Select Add storage.

2. Complete the details on the Request storage page, including:
   - The cluster you’re adding storage to
   - The type of storage (active or performance)
   - The new storage quantity

**Downsize storage**

On the storage details page for each cluster, a Downsize storage option appears alongside Total storage.

Before you submit a Downsize storage request, make sure your virtual servers won’t be affected by this change of state.
CHAPTER 4
YOUR MANAGED VIRTUAL SERVERS

BEFORE YOU CREATE A VIRTUAL SERVER

For security purposes, we suggest configuring a firewall in your public network before creating any virtual servers in your public network. Find instructions for adding and configuring firewall rules in our *Network and Security User Guide.*

Before you create virtual servers, make sure you have a way to access them from your local network, using either remote desktop software or a secure shell client.

VIEW YOUR SERVERS

The *Servers* page summarises the virtual servers on any of the cloud infrastructure products you’re subscribed to. This also includes servers in any of your data centre locations (Australia and globally) and those on both shared and dedicated compute.

This page does not display the dedicated resources of your service. See the previous chapter for details on viewing and managing blade and storage assets.

![Servers page screenshot]

Each of your managed virtual servers on dedicated compute displays with this icon:

![Managed virtual server icon]

Plus:

- The virtual server name defined by you
- IP address of vNIC 1 (not the management IP address). You’ll see the IP addresses when you click on the server

Select a server to view more details.

![Virtual server details]
CHAPTER 5
CREATE VIRTUAL SERVERS

Select **Add server** from the **Servers** page. Options for the type of server you can add will display, depending on your range of subscription(s). The circled options below are specific to the managed virtual server (dedicated) service.

**IF YOU SELECT VIRTUAL SERVER WITH SOFTWARE...**

You’ll arrive at a form where you can request a new virtual server(s) with the software you need. We’ll do the licensing and installation before handing control of your new virtual servers over to you. You’ll find our list of available software and installation requirements on this form plus the server configuration details and your choice of operating systems.

While it’s up to you to choose the right configurations for your business, if you need user sizing guidelines to help with your request for software on a new virtual server, see our **software technical specifications**.

Depending on the software you choose, the operating system options are:

- Windows Server 2008 R2 Enterprise (64-bit)
- Windows Server 2012 R1 Datacenter (64-bit)
- Windows Server 2012 R2 Datacenter (64-bit)
Also depending on the type of software you choose, you’ll need to provide some or all of the following configuration details:

- The number of virtual servers to install the software and/or its components onto
- The number of user licences
- Public or private network – if you select public network, you need to add the IP subnet and IP address
- Active Directory Domain Services domain name (for software that requires this, you’ll need to decide which domain you want your new server(s) joined to and ensure your Active Directory Domain Servers server is accessible from the network you request your virtual server(s) to be created on). You’ll also need to provide your domain administrator username and password (we recommend you change your password once your server(s) and its software are up and running).

Once you submit the form, we’ll install the software for you before handing control of your new virtual server(s) over to you. We do our best to install software on your new virtual server as quickly as we can, though due to the complexity it can take up to four business days.

Once you receive confirmation that your virtual server with software installation is complete you’ll need to:

- Create or configure firewall rules for the IP address(es) of the virtual server(s) we create for you
- Configure any virtual server backups, restores and snapshots you need
- Configure the software according to your business needs

Note: we do not provide any software support. You need to source any help you might need for set-up, configuration, usage, upgrades and ongoing management of the software.

Need to make any changes?

Email us if you want to change the number of users or CPU associated with your software.

Need to cancel your software?

Uninstall the software and email us when you’ve done so.

Want to remove a virtual server with software already installed on it?

Back up your data, delete the server and email us.

**IF YOU SELECT MANAGED VIRTUAL SERVER (DEDICATED)**...

You’ll arrive at the first of three steps in the virtual server configuration process. These are:

- Configure server
- Configure network
- Review

Using this option, you can create up to 10 virtual servers with the same configuration at a time, providing individual names for each server.

Once your virtual server(s) are active, the following are among some of the many service requests you can make:

- Resize your system disk or remove a disk
• **Increase data storage capacity**

• Modify the **power state**

• Request a **backup configuration** (then independently perform ad hoc backups and restores from backups for your virtual servers using the backup system).

### CONFIGURE MANAGED VIRTUAL SERVER(S)

To do this you’ll need to:

• Insert a name for each managed virtual server you add (a description is optional). Once each server is created, on the server’s details page you’ll see an additional virtual server ID defined by us. Refer to this second virtual server ID when submitting service requests or enquiries to us.

• Select an **operating system** and enter your operating system administrator username. On this service, you won’t receive the administrator account and password, but you will have administration rights.

• For a Windows machine, you will have a local administrator account; for a Linux machine your account can switch to root user using ‘sudo’, an application that provides user control and security enhancements to protect the root account and Linux system.

As well as administrator accounts, you will also see additional accounts on the servers used by us to administer your service. These are not to be modified or deleted.

• If the managed virtual server is connected to the public network and your firewall allows remote desktop software and/or secure shell client access, we recommend you create a sufficiently complex password.

• Select which configuration the server(s) is being added to (if you have more than one).

• Select a cluster to add the managed virtual server(s) to.

• Select the quantity of **CPU and RAM**.

• Once you’ve set up your managed virtual server, you can change the CPU and RAM. Note: decreasing from multiple CPU to single CPU may affect **high availability**.

• Resize and/or add virtual disks (optional) and select storage type. Each virtual disk can be between 100GB and 2TB in size. A maximum of 15 virtual disks can be added per service request.

### OPERATING SYSTEMS

Your managed virtual servers must be configured with one of our pre-defined operating system templates. You choose the operating system to suit your needs and we install it for you.

Various operating systems can be associated with a **cluster**, however some customers align operating systems to clusters to minimise operating costs, which are based on the number of physical CPUs on each blade in the cluster.

We currently support the following operating systems:

• Red Hat Enterprise Linux 5.x (64-bit)

• Red Hat Enterprise Linux 6.x (64-bit)

• Microsoft Windows Server 2003 Enterprise R2 (64-bit)

• Microsoft Windows Server 2008 Enterprise R2 (64-bit)

• Microsoft Windows Server 2012 Datacenter (64-bit)

• Microsoft Windows Server 2012 Datacenter R2 (64-bit)
OPERATING SYSTEM AND INFRASTRUCTURE PATCH MANAGEMENT

We actively monitor your compute environment and liaise with our vendors.

Our vendors provide VCenter patches – updates for reasons including, but not limited to, issues with stability and performance, vulnerabilities, supportability and weaknesses. Most patches are assumed to have been rigorously tested by the respective vendor under strict conditions; however the vendor cannot realistically test for all interoperability scenarios. This is why we test all selected patches that can potentially impact the platform.

We conduct two levels of testing and validation to ensure patch integrity and to mitigate virus damage from accidental execution of the file. The patch is then analysed through technical evaluation, a business impact assessment, security evaluation and a risk evaluation report providing a severity rating for how essential the patch is and how quickly it should be applied.

<table>
<thead>
<tr>
<th>SEVERITY</th>
<th>RISK</th>
<th>ACTION REQUIRED</th>
<th>RECOMMENDED TIMEFRAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>Unacceptable</td>
<td>ASAP</td>
<td>Deploy within maximum of 24 hours</td>
</tr>
<tr>
<td>Important or moderate</td>
<td>Marginally accepted</td>
<td>Consider action soon</td>
<td>Deploy within maximum of four months</td>
</tr>
<tr>
<td>Low</td>
<td>Acceptable</td>
<td>No immediate action</td>
<td>Deploy within maximum of twelve months</td>
</tr>
</tbody>
</table>

We always minimise the risk of disruption in applying the patch to your service. Part of the assessment is to determine whether an outage is necessary and, if required, when the best time is to restart your system.

Applying patches in the cloud infrastructure environment is subject to the following normal change management procedures:

1. Review each patch and approve it for the environment.
2. Send you a detailed report of patches/updates required for each of your servers with notification of the patching plan.
3. Schedule with you an agreed date to apply patches.
4. Perform pre-implementation checks (e.g. previous day backup completed, key Telstra services are up).
5. Perform the patches, confirm installation and perform post-implementation checks.
6. Notification sent to you advising you to test the application.
7. Notification sent to our support desk advising completion and alarming to be actioned.
CHAPTER 5  CREATE VIRTUAL SERVERS

CONFIGURE YOUR NETWORK

Choose which network in the virtual data centre to connect to. If you’re configuring a public network, you’ll be assigned a public IP address. For a private network, you can enter your own IP address, though it must be within your subnet range and not previously assigned. For more details, see the Network and Security User Guide.

REVIEW

Before submitting your request for a server(s), review all the details you’ve entered and make any changes.

MODIFY POWER STATE

Go to the Servers page and select the virtual server whose power state you want to modify.

Select the icon for a dropdown menu. Select the relevant power state modification you want to request us to make.
CHAPTER 6
GROUP VIRTUAL SERVERS

VIEW AND MANAGE GROUPS

Here, ‘groups’ and ‘grouping’ relate solely to the activities and view in the Cloud Services management console. Groups created here are not reflected as a resource group or any other in the virtualisation environment provisioned for you.

Groups allow you to organise your servers in any way you like (e.g. by function such as development, testing or production).

You can create and manage your own groups via the Servers section. A group can include servers on any of the cloud infrastructure products you’re subscribed to.

![Cloud Services Management Console](image)

1. Create a group icon
2. Server group name, defined by you

Find out how to:

- Create a group
- Move servers to groups
- Rename a group
- Delete a group

CREATE A GROUP

Initially, all of your managed servers are in Ungrouped.

From the Servers page, select the Create group icon to create a new group. Make sure you enter a unique name (i.e. not the same as an existing group).
A new empty group is created – ready for you to move your servers into it.

**MOVE SERVERS TO A GROUP**

Move individual or multiple servers to an existing group.

**Individual servers**

Select a server icon in any group, then hover over the arrow next to the name. Select *Move to...* from the menu to display the next *Move server to group* window (the *Move* link only displays if you’ve created more than one group).

**Multiple servers**

You can select multiple servers in *list* and *grid view*.

In *grid view*, select *Move servers* (the link displays if you’ve created more than one group).

A tick box displays next to the server names. Select one for each server you want to move.
Select a group from the *Move selected servers to* menu, then click *Move servers*.

In list view, select the tick box next to each server you want to move.

Select the *Move servers* link.

**RENAME A GROUP**

Select *Rename*. Enter a new name for the group, then select *Rename group*.

**DELETE A GROUP**

Select *Delete* link. A message displays asking you to confirm that you want to delete the group. Servers in a deleted group are moved back to *Ungrouped* (the ungrouped section can’t be deleted or renamed).
CHAPTER 7
MODIFY OR DELETE A VIRTUAL SERVER

CPU AND RAM
The CPU and RAM initially defaults to the minimum supported values of the operating system you select. If you decrease your CPU and/or RAM, the performance of the software installed on your virtual server may be impacted.

MODIFY CPU AND/OR RAM
1. From the Servers page, select the virtual server whose CPU/RAM you want to modify.
2. Select Modify CPU and RAM. The current CPU and RAM on the virtual server is displayed.
3. Select the new values (you may notice certain CPU/RAM combinations are not selectable if they’re not supported by your operating system) then click Update.

Note: if your virtual server is powered on, we’ll need to power it down to modify your CPU and RAM. We’ll notify you when this is scheduled to take place.

VIRTUAL SERVER DATA STORAGE
Each virtual disk that’s attached to a server supports a maximum of 2TB of data, though once it’s formatted the capacity is less than this.

SYSTEM DISKS
Each virtual server is created with a system disk for use by the operating system. The system disk can’t be removed. The default disk size depends on the operating system you choose:

- Linux® – 40GB
- Microsoft® Windows® Server 2008 – 60GB
- Microsoft® Windows® Server 2012 – 60GB

INCREASE THE SIZE OF A SYSTEM DISK
You can submit a request through the Cloud Services management console to increase (but not decrease) the size of the system disk after it has been created. The size can be increased in 10GB increments, from 10GB up to 2TB per disk. You also need to increase the system disk partition to be able to use the extra space. The disk partition size can’t be decreased.

1. From the Servers page in the Cloud Services management console, select the server whose system disk you want to increase. This expands the details and options you have for that virtual server.
2. Select the server’s Details tab.
3. In the virtual disks section, select Increase disk size next to the system disk details.
VIRTUAL DISKS

In addition to the system disk, each virtual server can have unlimited virtual disks ranging from 10GB to 2TB. The operating system can partition and format the disks as appropriate.

ADD A VIRTUAL DISK(S)/INCREASE DISK SIZE

In the Cloud Services management console, you can submit a request to add a new disk(s) or increase a disk’s size to create storage space for your virtual server.

From the Servers section, select the server whose disk details you want to update. This expands the details and options you have for that virtual server. Select the server’s Details tab.

Select Request disk to go to the Add disk form. From here you can create as many virtual disks as required per virtual server. You can also configure a backup from this section of the Cloud Services management console.

Choose a name for the virtual disk, storage type (active or performance) and disk space size.

To see the disk updates on your virtual server, you’ll need to partition and format your new disk in the operating system. You might need to re-boot the server.

REMOVE A VIRTUAL DISK

Removing a virtual disk deletes all data (including software) so, before you do, back up anything you wish to keep.

In the server’s Details tab, select Remove to submit a request to remove a disk. A confirmation form appears – accept. All information on the disk will be removed.

VNICS

By default, each virtual server is created with two virtual network interface cards (vNICs). The first vNIC is reserved by the Cloud Services support team for virtual server management purposes including configuration, application installation and backups. It’s also used for SSL VPN. The second vNIC is used to connect the server to your public (internet) or private network.

A third vNIC is added after the virtual server has been created if you dual-home the server to your public network (internet) and private network. Refer to the Network and Security User Guide for details.

DELETE VIRTUAL SERVER

Before submitting a request to us to delete a server, we recommend the following:

- Copy any data you’d like to keep
- Be aware that any software on the server is also deleted
  - If you have software purchased through us on the virtual server you’re deleting, email us when you delete the server and we’ll update your licence records
  - Check the licensing of any other software that’s installed on your server is not affected by its removal
- Remove the virtual server’s IP address from your firewall or load balancer configurations
- Submit a request to us via the Cloud Services management console to power off your virtual server (it needs to be powered off before it can be deleted)

In the individual server’s Details tab, select the icon to submit a request to delete a server.
A confirmation form appears.

When you submit a request to remove a virtual server, the following will appear on your server’s status:

When a server is deleted, if the server has backups, our backup team is notified to remove that server from backup schedules.
Server anti-virus protection is provided at specific IP addresses using both signature-based and heuristic detection. This provides an advanced and continually updated defence against viruses, Trojans and other malware. The service includes:

- 24/7 monitoring of operating systems and applications
- Rapid incident response
- Up-to-date security practices and procedures
- Service level agreements for policy changes and incident response

Our anti-virus service is implemented using McAfee SaaS Endpoint Protection. Anti-virus agents are installed on your physical or virtual servers. These agents are managed by McAfee’s centralised ePolicy Orchestrator. The anti-virus environment is scalable and fault-tolerant with the service configured to McAfee, operating system vendor and software vendor best practices.

The configuration is supported by our engineering and security teams and designed to protect your server so you can run your applications (note: most applications are catered for in the configurations).

The service runs real-time and scheduled (6AM daily) scanning. On-demand (manual) scanning is configured on the server for you to run. For customised configurations, contact us.
While operating system backups are set up automatically for your virtual server, to get started you first need to request a Telstra-scheduled backup configuration of your virtual server data (including database applications).

Once we’ve configured your backup, you can perform ad hoc backups and/or restores from backups directly from your virtual server using the installed backup system. Alternatively, you can submit a request to us to set up an ad hoc backup or restore for you (this service attracts a fee).

To configure, manage or remove your set-up, select Backup under the Infrastructure menu in the Cloud Services management console or by selecting the server (via the Servers page) and the Backup dropdown menu.

**BACKUP RETENTION**

<table>
<thead>
<tr>
<th>RETENTION PERIOD</th>
<th>FREQUENCY</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 week</td>
<td>7 daily backups</td>
</tr>
<tr>
<td>1 month</td>
<td>One month of daily backups</td>
</tr>
<tr>
<td>1 quarter</td>
<td>Three months of daily backups</td>
</tr>
<tr>
<td>1 year</td>
<td>Three months of daily backups</td>
</tr>
<tr>
<td>7 years</td>
<td>Three months of daily backups</td>
</tr>
</tbody>
</table>

**BACKUP MANAGEMENT TOOLS**

Two tools are available to help you manage your backups:

- Client software
- Administrator software

<table>
<thead>
<tr>
<th>CLIENT SOFTWARE</th>
<th>ADMINISTRATOR SOFTWARE*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client software is pre-installed on any virtual server</td>
<td>We pre-install the administrator software on your</td>
</tr>
</tbody>
</table>
running a *compatible operating system*. Plug-in software for databases will need to be installed by you if the database is not managed by us.

<table>
<thead>
<tr>
<th>Windows virtual server.</th>
</tr>
</thead>
</table>

To open the software in Windows, log in to your virtual server and click on the client icon in the taskbar. From here, selecting *Restore* or *Backup* will take you to the backup web interface.

To open the software, log in to your virtual server and select the administrator icon from your desktop. From here you can:

- Restore from a backup
- Create a non-scheduled backup
- View the backup activity log
- Produce backup reports

*If you only have Linux servers, you won’t have access to the administrator. You’ll need to use command lines to list all backups on a server and to initiate non-scheduled backups and restores. See Appendix E for command examples.

**NOTE THE FOLLOWING WITH YOUR BACKUP PLATFORM INSTALLATION**

- Do not activate your host using the backup software. We will do this.
- Enhanced backups and restores of database applications (Microsoft SQL Server, Exchange etc.) require your database administrator to set up access for backup. Refer to the relevant section below. Note: file system backups do not back up databases.
- Once your configuration is activated and a backup has been made, make sure you perform a test restore.
- We monitor alerts for failed backups. You can verify the status of your jobs, which you’ll receive in your daily email report.
- For restorations which require data that is over three months old contact us.

**HOST FILES**

Backup details are pre-configured in the host file for each of your virtual servers. Do not delete any backup host file entries. Host file entries correspond to your virtual data centre location.

**FIREWALL PORTS**

The following TCP ports should be open by default, unless you’ve previously installed a client-side firewall. If so, ensure these are open in both directions to the backup network:

- 27000
- 28000
- 28002
- 29000
- 7778
- 7779
CONNECTIVITY TEST

To test connectivity use the corresponding entry to your virtual data centre location:

- Sydney – telnet stlava02un01 28001
- Melbourne – telnet claava02un01 28001
- Perth – telnet welava01un01 28001
- Hong Kong – telnet honava01un01 28001
- Singapore – telnet sinava01un01 28001
- London – telnet lonava01un01 28001
- New Jersey – telnet njnava01un01 28001

ADMINISTRATOR LOGIN DETAILS

We sent your backup administrator login details to you after we set up your first backup. Passwords can be reset for a fee via the Cloud Services management console (we do not keep passwords).

You’re provided with one backup administrator username and password per location, with backup/restore rights. You cannot change the password, which is sent to you via encrypted email. We do not keep a record of passwords so please store yours safely.

To access the administrator, enter your user name, password, the virtual server’s domain name and administrator server.

Note: these login details are not the same as your Cloud Services management console login details.
## MANAGE YOUR BACKUPS

<table>
<thead>
<tr>
<th>RESTORE FROM A BACKUP</th>
<th>CREATE AN AD HOC BACKUP</th>
<th>CHANGE SCHEDULED BACKUP DIRECTORIES AND FOLDERS</th>
<th>CHANGE BACKUP RETENTION PERIODS</th>
</tr>
</thead>
<tbody>
<tr>
<td>To restore from a long-term backup, <strong>contact us</strong>. For short-term backups, select <strong>Backup and Restore</strong> using the administrator and follow the prompts. Or, select <strong>Restore</strong> in the client. You will need to check your backup reports to see if the restoration was successful.</td>
<td>Using the administrator, select <strong>Backup and Restore</strong> and follow the prompts. Or, select <strong>Backup</strong> in the client. To limit disruption to the backup servers, we recommend that you don’t create frequent non-scheduled backups.</td>
<td>To change the directories and folders for a scheduled backup, <strong>contact us</strong>.</td>
<td>Log in to the management console and go to <strong>Infrastructure &gt; Backups</strong></td>
</tr>
</tbody>
</table>

### AD HOC BACKUPS

A limited number of ad hoc backups can occur during the backup infrastructure maintenance window between 12PM and 6PM daily, when capacity is limited.

If your ad hoc backup cannot be performed at the time it’s requested, it will be performed in the next available window.
Ad hoc backups can be initiated at any time except during the backup infrastructure blackout window: between 6AM and 12PM daily.

**COMPATIBLE OPERATING SYSTEMS**

You can back up any of your virtual servers running *operating systems we currently support.*

**APPLICATION BACKUPS**

While configuring a backup, you can also back up the following applications:

- Microsoft SQL Server – you’ll need to identify the database location (e.g. C:\Program Files) and *backup type.*
- Microsoft SharePoint – provide the location of temporary files and your database
- Microsoft Exchange – provide database location and cluster virtual server (hostnames and IP addresses of relevant cluster(s)).
- Oracle – database name, location and *backup type* (full or transactional)
- Sybase – provide the instance name and Sybase OCS directory
- SAP on Oracle – provide the database location

**Application backup types**

- Full backup – always records the entire database (including all objects, system tables and data)
- Transactional backup – only records transaction logs, the serial records of all database modifications
- Differential database backup – records only the data that’s changed since the last full database back up

**EMAIL REPORTS**

You are emailed a daily, weekly and monthly backup report.
MORE DETAILS

Select an appendix link in the table heading for instructions on the following:

<table>
<thead>
<tr>
<th>APPENDIX A</th>
<th>APPENDIX B</th>
<th>APPENDIX C</th>
<th>APPENDIX D</th>
<th>APPENDIX E</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Install plug-ins for the following database backup software:</strong></td>
<td><strong>Backup and restore procedures for:</strong></td>
<td><strong>Find a backup server name</strong></td>
<td><strong>Restore backup file to an alternate server</strong></td>
<td><strong>Linux backup and restore command lines</strong></td>
</tr>
<tr>
<td>- Microsoft SharePoint Server</td>
<td>- Linux</td>
<td>- Microsoft SharePoint</td>
<td>- Oracle</td>
<td>- Sybase – for Windows and Red Hat</td>
</tr>
<tr>
<td>- Microsoft Exchange 2010 VSS</td>
<td>- Microsoft SQL Server</td>
<td>- Microsoft SharePoint</td>
<td>- Oracle</td>
<td>- Sybase – for Windows and Red Hat</td>
</tr>
</tbody>
</table>
CHAPTER 10
VIRTUAL SERVER SNAPSHOTS

A snapshot is a full system image copy of a virtual server. Snapshots are not recommended on databases, active directory servers and active directory integrated servers such as Microsoft Exchange Server. Refer to the VMware Knowledge Base for best practices for virtual server snapshots in the VMware environment.

A request for a virtual server snapshot can be made at any time through the Cloud Services management console.

You can make one request for a snapshot at a time for each virtual server. Each snapshot lasts until you choose to overwrite it by creating another snapshot.

Before taking a snapshot, check you have enough storage capacity in the server’s cluster.

Create a snapshot

To make a request to create a new snapshot, revert to the previous snapshot or to delete a snapshot, go to the Servers page, select the server you want to apply the Snapshot action to, then select the Snapshots tab.

Your snapshot is saved on one of the datastores in the cluster your virtual server belongs to. Before taking the snapshot, if we find you don’t have enough storage in your datastore, we’ll contact you to request that you provision more storage. To make the process easier, check that you have enough storage in your cluster for a snapshot to be taken.

Once you’ve taken a snapshot on a virtual server, the camera icon appears green and features a dropdown that displays the date and time the snapshot was taken and when it expires. You will also have options to Revert to snapshot, Create new snapshot or Delete snapshot.

Revert to snapshot
Requesting us to revert to a snapshot signals that you want to roll back a virtual server to its state when the most recent snapshot was captured. Before submitting a request, make sure you back up any data you wish to keep as changes made since creating your last snapshot will be lost. You won’t be able to use your server during the reversion and reversion times will vary according to server size.

Delete active snapshot

If you submit a request to delete a snapshot you won’t be able to revert your system configuration back to its previous point in time.
CHAPTER 11
SOFTWARE

You can install software that you’ve licensed on our virtual servers or, when you create a new virtual server, you can choose to add software from our range. We install the software we offer.

Our current range of software can be viewed in the Cloud Services management console when you select ‘Add virtual server with software’.

CLOUD READY

Want to know what software is compatible with your service? Our Cloud Innovation Centre team tests a variety of software products in our labs to see if they’re compatible with our services. For more information on whether a software package you wish to use is ‘cloud ready’, contact your Telstra representative.

MICROSOFT LICENCE MOBILITY

Thanks to our status as a Microsoft-authorized licence mobility partner, if you’re a Microsoft Volume Licensing customer covered by Microsoft Software Assurance you may be able to use your eligible Microsoft software licences on our cloud servers.

Licence mobility enables you to leverage your existing Microsoft licence investment on our cloud servers, making it easier to move to our Cloud Services.

The eligible application software licences are:

- Microsoft Dynamics® CRM Server
- Microsoft Exchange Server
- Microsoft Lync® Server
- Microsoft SharePoint® Server
- Microsoft SQL Server®

APPLYING FOR MICROSOFT LICENCE MOBILITY

STEP 1 – DETERMINE WHICH OF YOUR LICENCES ARE ELIGIBLE

View your licence status by logging in to the Microsoft Volume Licensing Service Centre and note which of the above eligible applications you’re licensed for. Typically, your IT or procurement department can access your licensing agreement details.

STEP 2 –VERIFY YOUR LICENCES WITH MICROSOFT

Under the Authorised Mobility Partner section of the form, you’ll need to write ‘Telstra Corporation Limited’ as your mobility partner and include our URL www.telstra.com and licensing email softwarelicensing@team.telstra.com. From there, wait for signed notification* from Microsoft before installing your software.

STEP 3 – INSTALL YOUR APPLICATION SOFTWARE
*If your licence(s) are eligible, Microsoft will email a counter-signed copy of the form both to you and us. If your licences can't be verified, Microsoft will return the verification form to you explaining why. You can make any necessary revisions and resubmit the form as many times as needed.

Remember, it's up to you to have the right licences to install and run software applications on your virtual servers. See our Responsibilities Guide and Customer Terms.

For all the details, see Microsoft Volume Licensing Software Assurance.
You can log in to the Cloud Services management console at any time to view usage and performance reports for your managed virtual servers. You can also manage performance thresholds and the way you’re notified of these (see ‘Server usage reports’ section below).

Log in to the Reports section of the Cloud Services management console to view usage for other services you might have, including:

- Virtual server (shared)
- Backups*
- Network and security (public IP addresses, firewalls, IPsec VPN tunnels)*
- Internet (including SMTP email relay)*

*Refer to the Reports section of the Account Management Guide for more details, including instructions on viewing the Cloud Services management console Activity log.

Note: Cloud Services management console reports do not detail monitoring levels for assurance of your managed virtual servers and virtualisation.
The *Usage* tab displays the CPU, RAM and disk space usage reports as well as HTTP response time reports. The data is updated each time you choose to view a report.

You have the option to view usage by day, week, month or year. The graphs display server resources used during the following periods:

- **Day** – the past 24 hours since midnight the previous day (AEST)
- **Week** – the past 8 days
- **Month** – the past 32 days
- **Year** – the past 13 billing months (including the current month).

The graphs show utilisation for each server resource:

- **Grey bars** – the percentage utilisation at each interval
- **Red bars** – the point at which utilisation reached current and past critical thresholds
- **Orange bars** – the point at which utilisation reached current and past warning thresholds.
Note: CPU utilisation is reported as the aggregated consumption of all your managed virtual servers’ CPUs.

Some graphs may show that a critical or warning threshold was exceeded even though the current threshold level is higher. Hover over the current threshold values to display the previous lower thresholds that applied during the same period.

You can also hover over the bars to display the exact percentage utilised at each point-in-time.

The reports show data from the past 13 months or as far back as your virtual server has been running if that’s less than 13 months.

You can request usage reports from more than 13 months ago by contacting us. If you email us outside of Australian business hours (AEST) we’ll get back to you the next business day.

### ADD A CONTACT

You can nominate contacts in your organisation to receive regular reports about your servers.

Add contacts via the Contacts section under Account.

Here you can:

- Modify and delete contacts
- Sort contacts using the Name column header.

Select Add new contact to add a new row to the contacts table.

Enter the person’s full name, email address and/or mobile phone number and choice of alert method, then click Save.
ASSIGN A CONTACT TO A SERVER

The next step is to assign (add) contacts to your servers and set the notification frequency.

Contacts are assigned to servers and performance indicators one at a time.

Select a server to view its details.

Use the server’s Thresholds & notifications tab to assign your contacts to the performance indicators.

Click the CPU, RAM, disk or HTTP response time section to reveal the settings table, then click Add contact to assign one of your contacts.

Select a name from your contacts list as well as the notification type (email, SMS or both), then click the Save button.

Clicking Modify under Actions takes you to the Contacts page where you first added the contact. From here you can edit or delete the contact (the notification settings for each server and performance indicator will be automatically updated).

You can also select the notification frequency (e.g. hourly) for each performance indicator. All assigned contacts will be notified of an exceeded performance threshold at the selected frequency interval.

VIEW AND MANAGE THRESHOLDS

You can specify critical and warning thresholds to monitor your managed virtual servers’ key performance indicators.

1. Select the server you want to specify performance thresholds for.
2. Select the *Thresholds & notifications* tab, which displays the server’s threshold and notification settings.

3. From here you can view and change the critical and warning thresholds for:
   - CPU utilisation
   - RAM utilisation
   - Disk space usage
   - HTTP response time.
VIEW AND MANAGE NOTIFICATIONS

Note: setting up notification contacts is only available to those with managed servers on dedicated compute. This function is not available for other infrastructure services, including Virtual Server (Dedicated) or Virtual Server (Shared).

You can set up automated SMS and email notifications from Telstra Cloud Services to alert your contacts as soon as a performance threshold is exceeded for one or more of your managed virtual servers.

Warning and critical notifications are sent to the server’s assigned contacts until you increase the performance threshold, the threshold is no longer being exceeded, or you change the notification settings.

Warning notifications stop when the server status changes to OK or are replaced by critical notifications when the server status changes to Critical.

Critical notifications stop when the server status changes to OK or are replaced by warning notifications when the server status changes to Warning.

Set up notifications in two steps:

- Add a contact
- Assign a contact to a server

You can also:

- View a notification log
- Stop notifications

NOTIFICATION LOG

The notification log can be accessed via an individual server’s Thresholds & notifications tab. The log displays your managed virtual server’s notifications (by ID and server status) over a three-month period.

The log shows which server the notification belongs to, which performance threshold was exceeded and the time the notification was sent.

Here you can:

- Filter the list by server status (Critical, Warning, Unknown, OK)
- Sort the notifications using the column headers.

You can also select the notification ID to view more details including which contact the notification was sent to.

STOP NOTIFICATIONS

To stop sending notifications to a contact, either:
• Delete the contact’s details in the Contacts section under Account

• Delete the contact from the server’s notification settings in the Thresholds & notifications tab under Infrastructure.
Follow instructions to install the plug-in for your service by selecting the relevant software:

- Microsoft SQL Server
- Microsoft SharePoint Server
- Microsoft SharePoint Server 2013
- Microsoft Exchange Server
- Microsoft Exchange Server 2010 VSS
- Sybase Windows and Red Hat
- Oracle on Enterprise Linux, Red Hat and Windows

**MICROSOFT SQL SERVER**

**PRELIMINARY STEPS**

**REQUIREMENT** | **MINIMUM/RECOMMENDED**
---|---
RAM | 512 MB (2GB recommended).
Hard Drive Space | 2GB permanent hard drive space for software installation. The Avamar SQL Server Client software also requires an additional 12 MB of permanent hard drive space for each 64 MB of physical RAM. This space is used for local cache files.
Network Interface | 10baseT minimum; 100baseT or higher recommended, configured with latest drivers for your platform.

**SET UP SQL**

In *Computer Management*, create new user with the name *svc_tbr* and a password.

Note: this account may already exist for NetBackup SQL, which can be used with Avamar as well. If so, skip to *Step 8.*
Once the account has been created, double-click on the account to open properties and select the Members Of tab. Type Administrators in the blank space and click OK.

Open and log in to Microsoft SQL Server Management Studio, expand Security and right click Logins. Select New Login.
Click Search.

Type svc_tbr in the blank space and click OK.
Select Server Roles (left pane), and tick the sysadmin check box.

Select Status (left pane), check that login has been enabled, then click OK.
Open *Computer Management*, then *Services*. Look for *Backup Agent* (Avamar) or *NetBackup Client Service* (Netbackup). Double-click to access its properties then select the *Log On* tab.

Select *This Account* and *Browse*, type `svc_tbr` then click *OK*. Type in the password you set up in Step 1 and click *OK*.

**INSTALL AVAMAR WINDOWS PLUG-IN**

Perform a test on file system backup to see if it works.

**INSTALL THE SQL SERVER BACKUP PLUG-IN**

1. Log in to the computer hosting the SQL Server.

2. Point your web browser at your backup server by typing the relevant backup platform URL e.g. `https://<avamar server name>`. You will be automatically redirected to the backup platform's secure web server. Depending on your browser security settings, a security alert dialog box might appear.

Your allocated backup server details would have been provided to you after you submitted a request to us to activate backups. See *Appendix C* for how to determine the backup server name on your server.

1. If a security alert dialog box appears, click *Yes* or *OK* to allow redirection to the backup secure web server.

2. Page down until the *Documents and Downloads* hyperlink is visible.

3. Click *Documents and Downloads*.

4. Click the appropriate operating system hyperlink for your client computer or workstation.
5. Double-click the corresponding install package `AvamarSQL-windowsx86-VERSION.msi` (32-bit) or `AvamarSQL-windows-x86_64-VERSION.msi` (64-bit).

Your browser will prompt you to either open the file in-place (on the server) or save it to your local computer or workstation. Either method will work. However, if you save the file to your local computer or workstation, you must open (double-click) that installation file to continue with this procedure.

6. Open the installation in place (on the server).

7. Follow the on-screen instructions.

8. Click Finish to complete the installation procedure.

**MICROSOFT SHAREPOINT SERVER**

The following are required to install and configure the backup plug-in for SharePoint:

- The standard backup plug-in has been installed and tested
- Microsoft SharePoint has been installed
- A folder has been created on the local disk of the SharePoint server for temporary backup files.
- The host with the installed backup plug-in must have a directory that is shared with enough space to accommodate the entire capacity of the MOSS Farm as a full backup.
- If the plan is to leverage both full and differential backups for restore, then adequate disk space on this host is required to recover both the full and differential export sets. Differential implies data changed since the last full backup.
- This host must also have credentials accessible by both the SQL Server service account and the MOSS Web server service account. The share permissions required for each account are:

<table>
<thead>
<tr>
<th>Domain Account</th>
<th>Grant Rights on Sharing Tab</th>
<th>Grant Rights on Security Tab</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL Server Database Service Account</td>
<td>Change, Read</td>
<td>Read, Write</td>
</tr>
<tr>
<td>Central Administrator Pool Account</td>
<td>Change, Read</td>
<td>All Except Full Control</td>
</tr>
<tr>
<td>Timer Service Account</td>
<td>Change, Read</td>
<td>All Except Full Control</td>
</tr>
</tbody>
</table>

**SET UP USER**

If this account is set to the SharePoint administrator, click OK.

If the Local System account is selected, select This account and type the SharePoint administrator account and password in the text boxes.
INSTALL PLUG-IN

For SharePoint 2013, note the special instructions below.

1. Log in to the computer hosting SharePoint.

2. Point your web browser at your backup server by typing the relevant backup platform URL e.g. https://<avamar server name>. You will be automatically redirected to the backup platform's secure web server. Depending on your browser security settings, a security alert dialog box might appear.

Your allocated backup server details would have been provided to you after you submitted a request to us to activate backups. See Appendix C for how to determine a backup server name on your server.

3. If a security alert dialog box appears, click Yes or OK to allow redirection to the secure backup web server.

4. Page down until the Documents and Downloads hyperlink is visible.

5. Click Documents and Downloads.

6. Click the appropriate operating system hyperlink for your client computer or workstation.
7. Double-click the corresponding *AvamarMoss* install package displayed below:

Install the plug-in by taking all the defaults during the installation e.g.
CHAPTER 13  APPENDIX A: INSTALL DATABASE BACKUP SOFTWARE (PLUG-INS)  55

Ready to install Backup Plugin for MOSS 2007

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

Installing Backup Plugin for MOSS 2007

Please wait while the Setup Wizard installs Backup Plugin for MOSS 2007.

Status:


SHAREPOINT SERVER 2013

On your SharePoint 2013 host, perform the following tasks:

Open your Services window.

Set the SharePoint VSS Writer Service with the following attributes:

- Startup Type = Automatic
- Logon User = set this to your SharePoint 2013 Windows account

Start the service by right-clicking it and selecting Start. E.g.

Install the Avamar for SharePoint agent.

Download and install the Avamar Agent for Sharepoint as described above.
When prompted for the type of installation, select the type of SharePoint installation you have i.e. either web/stand-alone or application/database server.

The screen above will result.

Select OK and complete your installation.

Open a DOS prompt and navigate to the folder below:

C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\15\BIN>

Enter the following two commands:

```
stsadm -o unregisterwsswriter
stsadm -o registerwsswriter
```

Re-start the Avamar service.

Open your Services window.
Select the Backup Agent service. Right click and select Re-start.

MICROSOFT EXCHANGE SERVER

Note: recovery of mailboxes requires an initial restore of the Microsoft Exchange database to a Recovery Storage Group. The mailbox can then be connected to the running database.

1. Log into the computer hosting the Microsoft Exchange server.
2. Point your web browser at your backup server by typing the relevant backup platform URL e.g. https://<avamar server name>. You will be automatically redirected to the secure backup web server. Depending on your browser security settings, a security alert dialog box might appear.

Your allocated backup server details would have been provided to you after you submitted a request to us to activate backups. See Appendix C for how to determine an backup server name on your server. For Exchange 2010, use Avamar Version 6.x or above.

3. If a security alert dialog box appears, click Yes or OK to allow redirection to the secure backup web server.
4. Page down until the Documents and Downloads hyperlink is visible.
5. Click Documents and Downloads.
6. Click the appropriate operating system hyperlink for your client computer or workstation.
7. Double-click the corresponding install package displayed below:

Your browser will prompt you to either open the file in-place (on the server) or save it to your local computer or workstation. Either method will work. However, if you save the file to your local computer or workstation, you must open (double-click) that installation file to continue with this procedure.
8. Open the installation in place (on the server). The Install Shield Wizard appears.

9. Follow the on-screen instructions.

10. Click Finish to complete the installation procedure.

**MICROSOFT EXCHANGE 2010 VSS**

Note: this is required for Exchange 2010 DAG configurations.

Download the *Avamar Exchange VSS* installation file. Install the plug-in as follows:
For granular/message level backups, select to install *Exchange GLR* and select a write cache folder:

![EMC Avamar Backup Plug-in for Exchange VSS Setup](image)

**Exchange GLR WriteCache Folder**

Click Next to use the default folder or click Browse to choose another.

**WriteCache Folder:**

C:\Program Files\avst\var\avfs\cache

![EMC Avamar Backup Plug-in for Exchange VSS Setup](image)

Completed the EMC Avamar Backup Plug-In for Exchange VSS Setup Wizard

Click the Finish button to exit the Setup Wizard.

**SYBASE WINDOWS AND RED HAT**

Ensure that the standard Avamar plug-in has been installed and tested successfully.

**Download installation package**

1. Log in to the computer onto which you want to install this software. Before downloading, ensure communications are working correctly by telnetting on port 28001 to your allocated backup server or one of the following that correspond to your server’s location:

   - **Sydney**: `$ telnet stlava02un01 28001`
2. The servers above are one of many backup servers that exist in each location. For each of your servers, it is important to download your software from your allocated backup server.

Your allocated backup server details would have been provided to you after you submitted a request to us to activate backups. See Appendix C for how to determine a backup server name on your server.

3. Point your web browser at your backup server by typing the relevant backup platform URL e.g. https://<avamar server name>. You will be automatically redirected to the secure backup web server. Depending on your browser security settings, a security alert dialog box might appear.

4. If a security alert dialog box appears, click Yes or OK to allow redirection to the secure backup web server. The Secure Log On page appears.

5. Page down until the Documents and Downloads hyperlink is visible.

6. Click Documents and Downloads. The Documents and Downloads page appears.

7. Click the correct operating system hyperlink for your client computer.

**WINDOWS**

![Web Access - Documents and Downloads](image)

Ensure the bitness of your Sybase installation matches the download selected. Download the file.
Select the install file and press Next.

Select Install when the set-up screen appears.
Complete the installation by copying file `<Avamar Install Path>\avs\bin\libsybase_avamar.dll` to your `<Sybase Install location>\ASE-15.0\lib`

**LINUX**

```
<table>
<thead>
<tr>
<th>Name</th>
<th>Last Modified</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>AvamarClient-linux-rhel-x86_64-6.1.101-87.rpm</td>
<td>11-Dec-2012 14:55</td>
<td>51.0M</td>
</tr>
<tr>
<td>AvamarDB2-linux-rhel-x86_64-6.1.101-37.rpm</td>
<td>11-Dec-2012 14:55</td>
<td>1.9M</td>
</tr>
<tr>
<td>AvamarRMAN-linux-rhel-x64_64-6.1.101-07.rpm</td>
<td>11-Dec-2012 14:55</td>
<td>1.6M</td>
</tr>
<tr>
<td>AvamarSAP-linux-rhel-x64_64-6.1.101-87.rpm</td>
<td>11-Dec-2012 14:55</td>
<td>3.5M</td>
</tr>
<tr>
<td>AvamarSybase-linux-rhel-x64_64-6.1.101-37.rpm</td>
<td>11-Dec-2012 14:55</td>
<td>1.8M</td>
</tr>
</tbody>
</table>
```

Ensure the bitness of your Sybase installation matches the download selected.

In the examples below, Sybase has been installed in the directory named `/var/sybase`

You’ll need to know the architecture of the Sybase application you’re running in order to download the correct plug-in file from the backup platform. If you’re unsure, you can confirm the architecture using the following command:
# file /var/sybase/ASE-15_0/lib/libsyb_tsm.so

The following sample text should be returned:

/var/sybase/ASE-15_0/lib/libsyb_tsm.so: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV),

Select and download the installation file for Sybase. Select the file name AvamarSybase-linux-type-x86-version.rpm

```
rpm -hi AvamarSybase-linux-type-x86-version.rpm
```

or

```
rpm -hi AvamarSybase-linux-type-x86_64-version.rpm
```

```
# 100%
# 100%
avagent Info: Stopping Avamar client Agent (avagent)...
avagent Info: Client Agent stopped.
avagent Info <0000>: Logging to /usr/local/avamar/var/avagent.log
avagent Info <5417>: daemonized as process id 17001
avagent Info: Client Agent started.
``` Installation complete

Create a symbolic link named *libsybase_avamar.so* in the Sybase ASE library directory
$SYBASE/$SYBASE_ASE/lib.

This points to the backup plug-in for Sybase library file (*libsybase_avamar.so*) in the
Avamar_installation_dir/lib directory.

For example:

```
# ln -s /usr/local/avamar/lib/libsybase_avamar.so /var/sybase/ASE-15_0/lib/libsybase_avamar.so
```

Confirm with:

```
# ls -l /var/sybase/ASE-15_0/lib/libsybase_avamar.so
```

Will return:

```
```

Copy and edit the *avsybase* script file, and add the Sybase OCS library path to the LD_LIBRARY_PATH path in the script. This resides in '/usr/local/avamar/bin' e.g.

```
LD_LIBRARY_PATH=${BASEDIR}/lib:/var/sybase/OCS-15_0/lib:${LD_LIBRARY_PATH}"
```
Enter the following command to activate the Sybase plug-in: /usr/local/avamar/bin/avregister

Enter the backup server name and domain name we provided to you when we activated your service.

Client Registration and Activation

This script will register and activate the client with the Administrator server.

Enter the Administrator server address (DNS text name or numeric IP address, DNS name preferred): AvamarServerName

Enter the Avamar server domain [clients]: AvamarDomainName

avagent.d Info: Stopping Avamar client Agent (avagent)...

avagent.d Info: Client Agent stopped.

avagent Info <0000>: Logging to /usr/local/avamar/var/avagent.log

avagent.d Info: Client activated successfully.

avagent Info <0000>: Logging to /usr/local/avamar/var/avagent.log

avagent Info <5417>: daemonized as process id 18347

avagent.d Info: Client Agent started.

Registration Complete.

Verify the configuration by entering the following command to check that the Sybase plug-in installation is complete:

# ./avsybase --version

The command should respond with:

version: 6.1.100-402

build date: Jun 13 2012 21:32:30

msg format: 13-10

SSL: TLSv1 OpenSSL 0.9.8r-fips 8 Feb 2011

Zlib: 1.2.3

LZO: 1.08 Jul 12 2002

platform: Linux

OS version: SLES-64

Processor: x86_64

ORACLE ON ENTERPRISE LINUX, RED HAT AND WINDOWS
INSTALL PLUG-IN

The standard backup plug-in first needs to be installed for the required platform.

Next, download the Avamar Oracle installation file for the platform required from an Avamar server.

INSTALL ORACLE PLUG-IN

RED HAT

For example:

```bash
root@lxdcbres01:/home/tdev# ls -l
total 1452
-rw-r--r--  1 tdev  tadmin  1477020 Dec 14 15:48 AvamarRMAN-linux-rhel3-x86-6.1.101-87.rpm
root@lxdcbres01:/home/tdev# rpm -ih AvamarRMAN-linux-rhel3-x86-6.1.101-87.rpm

avagent Info: Stopping Avamar client Agent (avagent)...
avagent Info: Client Agent stopped.
avagent Info <5241>: Logging to /usr/local/avamar/var/avagent.log
avagent Info <5417>: daemonized as process id 9807
avagent Info: Client Agent started.
Installation complete

Verify:
root@lxdcbres01:/home/tdev# rpm -qa | grep RMAN
AvamarRMAN-6.1.101-87
```

WINDOWS


Select the install file as in the sample below.
SET UP USER
This set-up must be completed by an Oracle database administrator (DBA). If an Oracle user account with SYSDBA privileges does not already exist, you must create one. This Oracle account (backupuser) is used to perform database backups and restores.

CONFIGURE HOT BACKUPS
To be completed by an Oracle database administrator. For example:

```
Prepare database for Hot Database Backups:

sqlplus "/ as sysdba"
```
SET-UP FOR RECOVERY

The following instructions are required to set up Avamar and RMAN for selective restores i.e. tablespace and file level recovery.

1. Set up avtar file
2. Create an Avamar folder to contain scripts i.e. /home/oracle/avamar/avtar-flags.txt

RED HAT LINUX

Create the following file:

```
--pidname=Oracle
--server=stlava02un01.tsb.avamar.com.au
--expires=30

Linux:
--pidnum=1002

Red Hat:
--logfile=/usr/local/avamar/var/rmanavtarbkup.log
--vardir=/usr/local/avamar/var/
--id=backup2@Cus
--ap=xxxxxxxx
--path=/Cus/cuspitsap001/cuspitzc02ssz02.hosting.telstra.com
--retention-type=daily,weekly
```

WINDOWS
Create a folder e.g. d:\oraexe\avamar

```bash
--pidname=Oracle
--server=claava02un01.dcb.avamar.com.au
--expires=1
--pidnum=3002
--logfile=C:\Program Files\avs\var\rman.log
--vardir=C:\Program Files\avs\var
--id=user1@/ztest/Windows
--ap=password
--path=/ztest/Windows/wsdcbres01
--retention-type=daily
```

**server** is the backup platform server (or administrator server) e.g. stlava03un01.tsb.avamar.com.au

**expires** is the backup retention in days i.e. 30 or 90 days

**id** is userid@domain of the client, e.g. backup2@Cus

**ap** is the password for the backup user name provided to you at activation

**SET PERMISSIONS**

**RED HAT LINUX**

- $ chmod 766 /usr/bin/avtar
- $ chmod 766 /home/oracle/avamar/avtar-flags.txt

**RED HAT**

- $ chmod 766 /usr/local/avamar
- $ chmod 766 /usr/bin/avtar
- $ chmod 777 /usr/local/avamar/bin/avtar
- $ chmod 766 /home/oracle/avamar/avtar-flags.txt

**CONFIGURE HOT BACKUPS**

To be completed by an Oracle database administrator.

For example:

Prepare database for hot database backups:

```sql
sqlplus "/ as sysdba"
```

SQL*Plus: Release 10.1.0.2.0 - Production on Wed Apr 6 14:19:12 2005
Copyright (c) 1982, 2004, Oracle. All rights reserved.
Connected to:
Oracle Database 10g Enterprise Edition Release 10.1.0.2.0 - Production With the
Partitioning, OLAP and Data Mining options

```
SQL> shutdown immediate;
Database closed.
Database dismounted.
ORACLE instance shut down.
SQL> startup mount;
```
ORACLE instance
ORACLE instance started.
Total System Global Area 171966464 bytes
Fixed Size 787988 bytes
Variable Size 144964076 bytes
Database Buffers 25168024 bytes
Redo Buffers 1048576
Database mounted
SQL> alter database archivelog;
Database altered.
SQL> alter database open;
Database altered.
SQL> exit
Disconnected from Oracle Database 10g Enterprise Edition Release 10.1.0.2.0

IF REQUIRED, CONFIGURE LOCK CHANGE TRACKING

To be completed by an Oracle database administrator. To perform incremental backups of an Oracle database, you must enable the Block Change Tracking feature. To determine whether or not Block Change Tracking is enabled, type the following from an SQL prompt:

select status from v$block_change_tracking;

The STATUS column shows whether or not Block Change Tracking is enabled. The FILENAME column contains the filename of the change tracking file.

Refer to your Oracle documentation for additional information about v$BLOCK_CHANGE_TRACKING.

To enable Block Change Tracking, perform the following:

1. Open a command shell.
2. Log into Oracle RMAN by using your Oracle user ID and password. The command prompt changes to:
   RMAN>
3. Connect to the Oracle database.
4. Type the following:

   alter database enable block change tracking using file
   '/app/oracle/change_file.fil';

   Oracle uses the change_file.fil file to track changes to datafiles.

TEST RMAN

To be completed by an Oracle database administrator. Create the following RMAN script:

Linux
run {
allocate channel c1 type sbt
PARMS="$SBT_LIBRARY=/usr/local/avamar/lib/libobk_avamar.so" format '%d_%U';
send "--flagfile=/home/oracle/avamar/avtar-flags.txt" "--bindir=/usr/local/avamar/bin";
release channel c1;
}

Windows
run {
    configure controlfile autobackup on;
    ALLOCATE CHANNEL ch1 TYPE sbt
    PARMs="SBT_LIBRARY=C:\Program Files\avs\bin\Libobk_avamar.dll ENV=(path=C:\Program
    files\avs\bin)";
    send '"--flagfile=D:\oraexe\avamar\avtar-flags.txt" "--bindir=C:\Program
    files\avs\bin"';
    RELEASE CHANNEL ch1;
}

Will return:

using target database controlfile instead of recovery catalog allocated
channel: c1
channel c1: sid=12 devtype=SBT_TAPE
channel c1: EMC|Avamar (avtar backup)
sent command to channel: c1
released channel: c1
Recovery Manager complete.

SAP WITH ORACLE ON RED HAT

Note that the Avamar SAP Agent is used. Ensure the same Filesystem and SAP plugin are used. The minimum
version is 6.1 SP1.

1. Point your web browser at the Telstra Backup Platform by typing the URL provided upon activation.
 Depending on your browser security settings, a security alert dialog box might appear e.g.
 http://<server name>

2. The Secure Log On page appears. Note: you don’t have to log in at this stage.

Scroll down until the Documents and Downloads hyperlink is visible and then follow the link. e.g.
’AvamarSAP-linux-rhel4_x86_64-6.1.100-402.rpm’.

3. Install using the downloaded ‘rpm’ file as displayed below;

```
root@rhel664test tdev[ ]# rpm -ih AvamarSAP-linux-rhel4-x86_64-6.1.100-402.rpm
Appending signature to /var/lib/rpm/avamarSAP-linux-rhel4-x86_64-6.1.100-402.rpm
Not yet signed.
Verifying... [ ok ]
Installing... [ ok ]
Write check header in /var/lib/rpm/AvamarSAP-linux-rhel4-x86_64-6.1.100-402.rpm
[ ok ]
Complete writing in /var/lib/rpm/AvamarSAP-linux-rhel4-x86_64-6.1.100-402.rpm
Cleaning up... [ ok ]
```

You may run /usr/local/avamar/bin/avregister to register and activate this
client with the Administrator server.

avagent Info <5241>: Logging to /usr/local/avamar/var/avagent.log
avagent Info <5417>: daemonized as process id 2066
avagent.d Info: Client Agent started.
CONFIGURE AVAMAR

In Red Hat, the path /var/avamar requires WRITE access by the ORAsid user account.

1. Copy the backint program from the SAP plug-in installation directory to the directory that contains the SAP BR*Tools to /usr/local/avamar/bin
2. Create Avamar Flag File: Log in to your SAP host as the SAP user. Create a directory with the name $home/avamar
3. Add the contents similar to the text below;

   ```
   --bindir=/usr/local/avamar/bin
   --sysdir=/usr/local/avamar/etc
   --vardir=/usr/local/avamar/var
   --id=AAAadmin@/AvamarDomainName
   --password=BBBBBB
   --account=/AvamarDomainName/AvamarSubDomainName/myhostname
   --server=AvamarServerName
   
   ```
   us/local/avamar is the location of the Avamar install.

   We supply the following details to you:
   - Avamar userid (e.g. AAAadmin)
   - Avamar password (e.g. BBBBBB)
   - AvamarDomainName (e.g. ComanyX)
   - AvamarSubDomainName (e.g. comstlsap001, comclasap001)
   - AvamarServerName (e.g. stlava01un01, clava01un01)

4. Edit your initDBSID.sap file and add the entries below;

   ```
   util_path = /usr/local/avamar/bin
   This path was used to install Avamar and should exist.
   util_par_file = /home/oraie0/avamar/avamar.txt
   This is the full path of the Flag File created above.
   
   Note: for restore operations, perform the steps below:
   - Comment out util_par_file
   - Perform the restore(s)
   - Comment in util_par_file
   
   ```

CONFIGURE ORACLE

Check the status of the log mode by using the following procedure:

```
> sqlplus /Nolog;
SQL*Plus: Release 11.2.0.2.0 Production on Mon Mar 4 14:23:46 2013
Copyright (c) 1982, 2010, Oracle.  All rights reserved.
SQL> connect / as sysdba;
Connected.
SQL> select NAME,LOG_MODE from v$database;
NAME     LOG_MODE
--------- -----------
IU4       ARCHIVELOG
If Archivelog is not set as the log_mode), then;
```
Set “sysdba” privileges to the database user being used for backup and restore. For example, if the user is “sapuser”:

```
SQL> grant sysdba to sapuser;
SQL> select * from v$pwfile_users;
```

<table>
<thead>
<tr>
<th>USERNAME</th>
<th>SYSDB</th>
<th>SYSOP</th>
<th>SYSAS</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYS</td>
<td>TRUE</td>
<td>TRUE</td>
<td>FALSE</td>
</tr>
<tr>
<td>SAPUSER</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>SYSTEM</td>
<td>TRUE</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
</tbody>
</table>
This appendix outlines backup and restore procedures for:

- Microsoft Windows filesystem
- Microsoft SQL Server
- Microsoft SharePoint Server
- Microsoft Exchange Server
- Linux – including Oracle, Red Hat, SUSE, Ubuntu and CentOS
- Sybase – for Windows and Red Hat

MICROSOFT WINDOWS SERVER AND FILESYSTEM BACKUPS

AD HOC BACKUPS

Click the Backup & Restore tab, the Backup & Restore window appears.

Click the Select for Backup tab.

Select a client in the clients tree. A list of the clients files, folders and directories is displayed to the right of the client’s tree. Place a check mark next to the directories or files you wish to select for backup.

Select one or more directory and/or files.
Select Actions > Backup Now or click the toolbar icon shown immediately to the left. The On Demand Backup Options dialog box appears.

Review your backup settings. Clicking Cancel returns you to the Backup and Restore window where you can modify your backup selections.

If you want to change your backup retention setting, select the Retention period. To have this backup automatically deleted after a specific period of time - type the number of days, weeks, months or years. Set the retention period to either 30 days or 3 months.

Select None for the encryption method.

Select More Options. If there is an entry for a hostname in the field Store backup on Data Domain system select it as shown in the sample below. Click OK.
Click OK again. The On Demand Backup Options dialog box closes and the following status message appears: Backup initiated.

Click OK and monitor it from the Activity Monitor.

GROUP BACKUP

A backup group is a set of backups for one or more servers with a similar profile.

Click the Policy Management tab.

Click the Groups tab. Select the group you want to backup. Right mouse click, and choose Back Up Group Now.

Only select a group backup if you want to back up all the clients in the group.
The following status message appears: *Backup initiated*. Click *OK* and monitor it from *Activity Monitor*. 

![Activity Monitor Screenshot](image)
RESTORE FROM A BACKUP

The Backup and Restore window provides two alternative ways to locate and select a backup stored on the server. You can search for a backup by:

- Calendar date
- Content

RESTORE BY CALENDAR DATE

You can locate a stored backup by the date it was created.

Select Backup and Restore followed by the Select for Restore tab.

Select a client in the clients tree, then click the Select for Restore tab.

Click the By Date tab. A calendar will appear for locating backups stored on the backup platform. Dates highlighted in yellow on the calendar, indicate that a backup was performed on that date.

Selecting a highlighted backup date on the calendar populates the backups list immediately to the right of the calendar. Selecting one of the backups from the list, populates the contents list directly below the Backup History pane.

In the Backup History pane, browse to a valid backup date in the calendar (highlighted in yellow).

Select the backup from which you want to restore directories, folders or files.
Select Actions > Restore Now. The Restore Options dialog box appears.

Review your restore settings. Clicking Cancel will return you to the Backup and Restore window where you can modify your restore selections. Restore Destination Choices allows you to specify which client and top-level (root) directory will receive the restored files.

If you want to change your restore destination choices, select or type one of the following options:

- **Restore everything to its original location**
  
  This is the default destination — all files are restored to the original client in the original top-level (root) directory.

- **Restore everything to a different location**
This option allows you to **restore to an alternate virtual server** (a target directory other than the origin of the backup).

**MICROSOFT SQL SERVER BACKUPS**

Click the *Backup and Restore* tab, the *Backup and Restore* window appears.

Click the *Select for Backup* tab.

Select a client in the clients tree. A list of the client’s files, folders and directories is displayed to the right of the client’s tree. Placing a check mark next to a directory or file selects it for backup.

Select one or more directories and files.

If you want to change your backup retention setting, select the *Retention period*, if you want this backup to be deleted from the backup server after a specific number of days, weeks, months or years, type the number of days, weeks, months or years. Set the retention period either 30 days or 3 months.

Select *None* for the encryption method.

Select *More Options*. If there is an entry for a hostname in the field *Store backup on Data Domain system* select it as shown in the sample below. Click *OK*.

Click *OK* again. The On Demand Backup Options dialog box closes and the *Backup initiated* status message appears:

Click *OK* and monitor it from activity monitor.
Note: to perform a tail-log backup, the database must be online and using either the full or bulk-logged recovery model. To perform a point-in-time restore, the database must be using the full recovery model. As a result, you cannot perform either a tail-log backup or a point-in-time restore of system databases such as the master, msdb, and model databases because those databases use the simple recovery model.

To restore to a specific point in time, you must provide the transaction date and time or named mark to recover to from the SQL Server transaction log. The SQL Server documentation on the Microsoft website provides details on how to access transaction log information.

The point in time that you are restoring to must be after the finish time for the most recent full backup. In addition, if the point in time is before the start time of the most recent transaction log (incremental) backup, then a tail-log backup is not required. However, a tail-log backup is required if the point in time is after the most recent transaction log backup.

When you specify the point in time for restore, do not specify the start time of the selected transaction log backup if it is not the last backup in the backup sequence. Otherwise, the restore fails and a tail-log backup does not occur even if the Log Tail Backup option is selected.

Log in to the Avamar administrator console.

1. Select a client in the clients tree, click Select for Restore tab.
2. Click the By Date tab. Clicking the By Date tab displays a browsable calendar for locating backups in the Avamar server. Dates highlighted in yellow indicate that a backup was performed on that date. Selecting a valid backup date on the calendar populates the backups list immediately to the right of the calendar. Selecting a backup populates the contents list directly below the Backup History pane.
9. In the Backup History pane, browse to a valid backup date in the Calendar (highlighted in yellow).
10. Select the backup from which you want to restore directories, folders or files.

Select Actions > Restore Now, the Restore Options dialog box appears. Review your restore settings, select None for Encryption method.

Full backups are f-0 files, differential backups are d-n files, and transaction log (incremental) backups are i-m files.

If you are restoring from a transaction log or differential backup, select the database backup file that corresponds to the date and time to which you want to recover.

During the restore process, the backup service automatically restores any necessary data from the full backup, then restores and applies the intervening backup files as necessary. In other words, you do not need to select the full backup in addition to the transaction log or differential backup.

Select the most recent backup file if you plan to perform a tail-log backup and recover to a point in time since that last backup. A tail-log backup only includes transactions that have not yet been included in a backup.
Select the Restore Destination. See Appendix D for how to restore to an alternate server.

Select More Options

Select Show Advanced Options
Specify either the point in time or the named mark to recover to.

To recover to a specific point in time, specify the date and time in yyyy-mm-ddThh:mm:ss format in the Point-in-Time text box. For example, 2011-02-25T14:15:45 is February 25, 2011 at 2:15:45 p.m.

To recover to a named mark, specify the mark in the Mark name text box.

Note: specify either a point in time or a named mark, but not both. If you specify both, then the restore fails to complete and an error message is written to the log file.

If you specified a mark and named marks are not unique in the transaction log, then use the After date/time text box to locate the mark to recover to. The recovery process stops at the first mark with the specified name, exactly at or after the specified date and time. Specify the date and time in yyyy-mm-ddThh:mm:ss format.

Click OK. The Restore Options dialog box closes and the Restore initiated status message appears.

Monitor it from the activity monitor.
MICROSOFT SHAREPOINT SERVER

BACKUP

In the Backup and Restore tab, select Backup.

Select the SharePoint components to backup:

Right click and select Backup Now.

RESTORE

In the Backup and Restore tab, choose the Select for Restore tab. For example:

Select the Sharepoint option you wish to restore.
Right click and select *Restore Now*.

---

**CHAPTER 14  APPENDIX B: BACKUP AND RESTORE PROCEDURES FOR FILESYSTEM AND DATABASE SOFTWARE**

87
Select the *Restore type*, either *Overwrite* or *New*.
MICROSOFT EXCHANGE SERVER

BACKUPS

- Navigate to the backup pane
- Select the host and Exchange component required for the backup
- Select Actions > Backup Now.

For example:
Monitor activity using the Activity Monitor. For example:

RESTORE

Before performing a database restore, carefully review all restore options. If you do not want to overwrite the database, restore the database to a Recovery Storage Group (RSG) instead by selecting the Restore into Recovery Storage Group option from the Restore Options dialog box in the administrator.

Note: at the time of backup, the restore target Exchange server must have the same version and service pack level as the source Exchange server.

EXCHANGE SERVER 2007 DATABASE MOUNTING AFTER RESTORE

Before starting a restore, Avamar must dismount all databases within a storage group, whether they are all part of the restore or not. When the restore is completed, Avamar will attempt to mount all existing databases in the storage group whether they were previously mounted or not. Avamar will not attempt to mount databases that do not exist on disk, even if they exist within the Active Directory.

Selective restore of databases may fail if done from an older backup.

The restore of selected databases may fail if done from an older backup after a restore of that database has been done with a newer backup. If this occurs, you can delete the restore.env file created in the log folder path along with all the log files in that path, and rerun the restore.
ADDITIONAL NOTES ABOUT RESTORING TO AN EXCHANGE RDB OR RSG

In Exchange Server 2010 and Exchange Server 2007, you can recover a database to a separate storage group or database without disrupting your active production databases and servers. Once you have recovered the database, you can explore and select individual mailboxes to recover to your production server while it is online. In Exchange Server 2010, this capability is provided by the RDB feature. In Exchange Server 2007, this capability is provided by the RSG feature. The Avamar Exchange VSS Client provides the Windows Exchange VSS plug-in for recovering to an Exchange Server 2010 RDB or Exchange Server 2007 RSG.

When you use the restore to a RDB or RSG feature, always delete the existing RDB or RSG and then create a new clean RDB or RSG. If you are performing a directed recovery, delete the existing RDB or RSG on the original server as well as the RDB or RSG on the target server.

The restore process should be managed by the Exchange Administrator. The procedure involves:

In the Backup and Restore tab, select Restore.

Highlight the date of the backup.

Select Plug-In Windows Exchange Database.

Select the Exchange component to restore. The example above has: 19 Dec 2010, Second Storage Group

Select Actions >> Restore Now

The Restore Options panel will display:
Select the *Host* to direct the restore operation.

Select *More Options*:

- Select the options required to perform the recovery as in the example above
- Select *OK* and the recovery will commence

Use the *Activity Monitor* to view the process of the operation
Specify a setting that will allow this database or all databases to be overwritten by the restore, using one of the two following methods:

To specify to allow overwrite of just the database you actually want to restore, in the Restore Command Line Options dialog box, leave the Allow database overwrite checkbox cleared, and then in Exchange Management Console, select the This database can be overwritten by a restore option in the recovery options for the database you want to restore. This allows you to set Allow database overwrite for the databases that were selected for restore.

OR

To specify to allow overwrite of all databases when you perform a restore, in the Restore Command Line Options dialog box, select the Allow database overwrite option.

Note: If you select the Allow database overwrite option and accidently select a database to be restored, it will be overwritten. By default, when you first open the Restore Command Line Options dialog box, this setting is not selected.

Select or type other options as needed, and then click OK when done.

LINUX

This section includes the procedure for the platforms listed below. The administration console can be used to manage these platforms:
• Oracle Linux
• Red Hat
• SUSE
• Ubuntu
• CentOS

MANAGE YOUR SYSTEM FROM THE COMMAND LINE

The avtar program is a command-line backup and restore program used to:

• Backup files and directories
• Delete an existing backup
• Extract and restore files or directories from a previous backup
• List the labels and dates of backups, or list the names of files and directories in a backup
• Validate a backup to ensure that data can be extracted.

AVTAR SYNOPSIS

avtar {{ --create | -c} | --delete | {--extract | --get | -x} | {--list | -l} | --backups | --validate} FILE1 [FILE2 ...] DIR1 [DIR2 ...]

One (and only one) of the following commands must be supplied on each command line:

--create or -c creates a new backup. Typically, you should include a list of files, directories or a path you want to back up. If you do not specify which files, directories or a path to backup, your entire local filesystem is backed up.

--delete deletes an existing backup.

Backups can only be deleted one at a time.

--extract or -x restores (extracts) files or directories from a previous backup.

--list or -l lists the contents of a backup. When used with the --verbose option, it returns file and directory permissions, size, creation date and time, as well as the file or directory name.

--backups lists all backup names and when they were created by a specific user account.

--id specify the full path for the user id, this will be provided by Telstra operation team with the password.

You need the login name, password and domain Avamar host name to log in using SSH. These details are provided by us.

AVTAR EXAMPLES

Show backups for user id user1@here:

• user1 is the user name provided by Telstra
• z-test is the primary domain name
• linux is the sub-domain name
- *lxtsbres01* is the host name
- *password* is your Avamar domain password

```
root@lxtsbres01:~# /usr/local/avamar/bin/avtar --backups --id=user1@/z-test/linux/lxtsbres01

avtar Info <5551>: Command Line: /usr/local/avamar/bin/avtar --vardir=/usr/local/avamar/var --bindir=/usr/local/avamar/bin --sysdir=/usr/local/avamar/etc --backups --id=user1@/z-test/linux/lxtsbres01

Password:

avtar Info <5552>: Connecting to Server (tsbava01un01.tsb.avamar.com.au)

avtar Info <5583>: Login User: "user1", Domain: "default", Account: "/z-test/linux/lxtsbres01"

avtar Info <6509>: Successfully logged into Server

avtar Info <7338>: Backups for /z-test/linux/lxtsbres01 as of 2010-04-22 13:01:13 EST

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Seq</th>
<th>Label</th>
<th>Size</th>
<th>Plug-in</th>
<th>Working directory</th>
<th>Targets</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010-04-09</td>
<td>13:48:25</td>
<td>1</td>
<td>linuxfs</td>
<td>1270784006846</td>
<td>38490839K Unix</td>
<td>/var/avamar</td>
<td></td>
</tr>
</tbody>
</table>

avtar Info <5314>: Command completed (exit code 0: Success)#

**Restore /var/log to target /restore1/avamar:**

```
usr/local/avamar/bin/avtar -xv --target="/restore1/avamar" /var/log --id=user0@/z-test --acct=/ztest/linux/lxtsbres01

avtar Info <5551>: Command Line: /usr/local/avamar/bin/avtar.bin --vardir=/usr/local/avamar/var --bindir=/usr/local/avamar/bin --sysdir=/usr/local/avamar/etc -x -v --target="/restore1/avamar" /var/log --id=user1@/z-test/linux/lxtsbres01

Password:

avtar Info <5552>: Connecting to Server (tsbava01un01.tsb.avamar.com.au)

avtar Info Enter password:password

avtar Info <5583>: Login User: "user1", Domain: "default", Account: "/z-test/linux/lxtsbres01"

avtar Info <6509>: Successfully logged into Server

avtar Info <5295>: Starting restore at 2010-04-22 13:06:47 EST as "root" on
```
"lxtsbres01" (2 CPUs) [5.0.101-32]

avtar Info <5949>: Backup file system character encoding is UTF-8.

avtar Info <8695>: Backup from Linux host "/z-test/linux/lxtsbres01" (lxtsbres01) with plug-in 1001 - Linux Filesystem

avtar Info <5538>: Backup #1 label "linuxfs-1270784006846" timestamp 2010-04-09 13:48:25 EST, 44,171 files, 36.71 GB

avtar Info <5291>: Estimated size for "/var/log" is 15.56 MB

avtar Info <5260>: Restoring files from "/var/log" to directory "/restore1/avamar".

/restore1/avamar/Xorg.0.log
/restore1/avamar/Xorg.0.log.old
/restore1/avamar/acpid
/restore1/avamar/anaconda.log
/restore1/avamar/anaconda.syslog

Etc......

Etc...

avtar Info <5267>: Restore of "/var/log" completed

avtar Info <7875>: Restored 15.56 MB from selection(s) with 15.56 MB in 71 files, 6 directories

avtar Info <6090>: Restored 15.56 MB in 0.06 minutes: 14.28 GB/hour (66,734 files/hour)

avtar Info <7833>: Finished at 2010-04-22 13:06:47 EST, Elapsed time: 0000h:00m:03s

avtar Info <6608>: Not sending wrapup anywhere.

avtar Info <5314>: Command completed (exit code 0: Success)

#

Backup /var/log:

root@lxtsbres01:~ # /usr/local/avamar/bin/avtar -cv /var/log --id=user1@/z-test/linux/lxtsbres01

avtar Info <5551>: Command Line: /usr/local/avamar/bin/avtar.bin --vardir=/usr/local/avamar/var --bindir=/usr/local/avamar/bin --sysdir=/usr/local/avamar/etc -c -v /var/log --id=user1@/z-test/linux/lxtsbres01
Password:

avtar Info <5946>: File system character encoding is UTF-8.

avtar Info <7508>: Starting back up at 2010-04-22 13:09:40 EST as "root" on "lxtsbres01" (2 CPUs) [5.0.101-32]

avtar Info <5730>: Entering include/exclude rules.

avtar Info <5552>: Connecting to Server (tsbava01un01.tsb.avamar.com.au)

avtar Info <5583>: Login User: "user1", Domain: "default", Account: "/z-test/linux/lxtsbres01"

avtar Info <5550>: Successfully logged into Server (Compression enabled)

avtar Info <7513>: Back up of "/var/log" on server "tsbava01un01.tsb.avamar.com.au" for /z-test/linux/lxtsbres01

avtar Info <5586>: Loading cache files from /usr/local/avamar/var

avtar Info <6426>: Done loading cache files

/var/log/boot.log
/var/log/boot.log.1
/var/log/boot.log.3
/var/log/boot.log.2
/var/log/boot.log.4
/var/log/cron
/var/log/cron.3
/var/log/cron.1
Etc....

avtar Info <5163>: Backup complete, wrapping-up session with Server

avtar Info <5156>: Backup #2 timestamp 2010-04-22 13:09:41, 72 files, 9 directories, 15.80 MB (61 files, 1.532 MB, 9.70% new)

avtar Info <7539>: No label, no scheduled expiration

avtar Info <6083>: Backed-up 15.80 MB in 0.08 minutes: 12 GB/hour (55,807 files/hour)

avtar Info <5587>: Updating cache files in /usr/local/avamar/var

avtar Info <7833>: Finished at 2010-04-22 13:09:41 EST, Elapsed time: 0000h:00m:04s

avtar Info <6608>: Not sending wrapup anywhere.
ORACLE

ON DEMAND AND GROUP BACKUP

Select the group to back up and select Backup.

Select Activity Monitor to view the results.

RESTORE PROCEDURE

Oracle database operator to prepare database, depending on the type of restore operation being performed.

RESTORE FROM LATEST BACKUP

The following is an example in /home/oracle/avamar/restore.rcv
run {
allocate channel c1 type sbt
PARMS="SBT_LIBRARY=/opt/AVMRclnt/lib/libobk_avamar.so";

send "flagfile=/home/oracle/avamar/avtar-flags.txt" "bindir=/opt/AVMRclnt/bin";
restore datafile "/u02/oradata/PDCBRC01/tools01.dbf";
recover datafile "/u02/oradata/PDCBRC01/tools01.dbf";
release channel c1;
}

Start the restore, for example:

$ rman target / @/home/oracle/avamar/restore.rcv

RESTORE FROM PREVIOUS BACKUP

The example below will restore a datafile from a backup taken 21 Dec 2010.

List backups in RMAN and obtain TAG.

oracle@tsblabvcs:../avamar:PDCBRC01> rman target /
Recovery Manager: Release 9.2.0.5.0 - Production
Copyright (c) 1995, 2002, Oracle Corporation.  All rights reserved.
connected to target database: PDCBRC01 (DBID=3652467607)
RMAN> list backup;
BS Key Type LV Size       Device Type Elapsed Time Completion Time
------- ---- -- --------- ----------- ---------------
6638    Full 211M       SBT_TAPE      00:00:33  21-DEC-10
BP Key: 6638   Status: AVAILABLE   Tag: TAG20101221T114943
       Piece Name: PDCBRC01_gkm041un_1_1
List of Datafiles in backup set 6638
File LV Type Ckp SCN   Ckp Time Name
---- -- --------- ------- ----
1    Full 182224026  21-DEC-10 /u02/oradata/PDCBRC01/system01.dbf
2    Full 182224026  21-DEC-10 /u02/oradata/PDCBRC01/undo01.dbf
Create RMAN script as in the example below, adding the TAG:

```sql
run {
allocate channel c1 type sbt
PARMS="SBT_LIBRARY=/opt/AVMRclnt/lib/libobk_avamar.so";
send '"--flagfile=/home/oracle/avamar/avtar-flags.txt" "--bindir=/opt/AVMRclnt/bin"';
restore datafile "/u02/oradata/PDCBRC01/tools01.dbf" from tag='TAG20101221T114943';
recover datafile "/u02/oradata/PDCBRC01/tools01.dbf";
release channel c1;
}
```

Start the restore, for example:

```
$ rman target / @/home/oracle/avamar/restore.rcv
```

**SYBASE FOR WINDOWS AND RED HAT**

The administrator console is the recommended tool for restoring Sybase structured application data to a Linux server.

Log in to the administrator console.

Select the *Backup & Restore* tab.
Select the host to backup.

In the *Browse for Files, Folders, and Directories* pane, select *Sybase ASE*. 
Enter the information as per the sample above.

For the OCS library directory:

For Windows, enter the `\OCS library path\dll`

For Red Hat, enter `/ocs_library_path/lib`
The database will be displayed.

Select the database to backup. Select *Actions >> Backup Now.*

Select the *Activity Monitor* tab to view the display of the backup operation.

You can double-click the job to obtain a detailed status of the log.
Select a retention period that you are set up to use i.e. 30 or 90 days.

For Encryption Method, select None.

Select More Options. If there is an entry for a hostname in the field Store backup on Data Domain system select it as shown in the sample below. Click OK.

Click OK again and the backup will commence.

**RESTORE**

Select the Backup & Restore tab.

Select Select to Restore.

Highlight the server in the list down the left column on the window.

Using the calendar, select the date you wish to restore from.
Select the database to restore.

Select Actions > Restore.

Select More Options.

Enter the details for the fields labelled:

- Sybase installation directory (e.g., /sybase)
- OCS library directory (e.g., /sybase/OCS-15_0/lib)
- Sybase username (e.g., sa)
- Sybase user password

Select OK to start the restore.
There are a few ways to retrieve a backup server name.

Firstly, check your records – the server name should have been provided to you after you submitted a request to us to activate backups.

If backups are already running on your server, you can check your daily report for backup server details.

Otherwise, enter the following details for the relevant service, which also shows what backups are working on your server.

**LINUX SERVER**

```
#service avagent status
```

**WINDOWS SERVER**

1. Click the Avamar icon in the task tray.
2. Select Additional Info...
3. An About Avamar Client box appears – view the Avamar Server details.
Your restore target does not have to be the same virtual server the backup was originally created from.

You can restore a stored backup file to any type of Telstra virtual server that shares the same virtual data centre location as the virtual server the backup originated from.

You can restore to an alternate virtual server from either:

- A long-term backup
- A short-term backup

The target virtual server you are restoring to may need to be redirected to the backup platform containing the data to be restored. A virtual server can only be connected to one backup platform at a time.

**Note:** performing a single-directory restore to an alternate virtual server will only restore the contents of the directory. The original parent directory is not restored as part of this operation. However, if you restore two or more directories to an alternate virtual server, then the original parent directories will be restored along with the contents of those directories.

**RESTORE A LONG-TERM BACKUP TO ALTERNATE VIRTUAL SERVER**

To restore from a long-term backup, you’ll need to contact us to specify details including:

- The virtual server the backup was created from
- The backup files/folders you want to restore
- The alternate backup target virtual server
- The directory location you’d like the files restored to

We perform all restores from long-term backups. We’ll identify and advise you if a redirected restore is required when you make your backup request. A redirected restore could cause a temporary backup service interruption.

**PREPARE TO RESTORE A SHORT-TERM BACKUP TO ALTERNATE VIRTUAL SERVER**

You can check the backup platform that a virtual server is connected to at any time by following the initial instructions to change your backup platform connection.

To allow us to perform a restore to an alternate target, your target virtual server may need to be temporarily redirected to the backup platform where your chosen backup file(s) are stored.
If so, and you’re restoring to a *managed virtual server (dedicated)* then we’ll take care of the platform redirection for you.

We’ll advise you by email if you need to perform a redirection for a *virtual server (dedicated) or virtual server (shared)* restore target. In this case, you’ll need to *change your backup platform connection*.

**POSSIBLE BACKUP SERVICE INTERRUPTION**

If you have scheduled backups configured on your restore target virtual server, your backup service could be interrupted.

A virtual server can only be connected to one backup platform at a time. Daily scheduled backups will not perform successfully from your target virtual server while it’s temporarily redirected to a different backup platform.

If your redirected target is a *managed virtual server (dedicated)*, we’ll email you to let you know when the redirected restore is complete, and your scheduled backups will resume on your target virtual server.

If your redirected target is a *virtual server (shared) or virtual server (dedicated)*, we’ll advise you when the restore is complete. The scheduled backup service on your target virtual server will only resume when you *change* your backup platform connection to its original address.

**CHANGE A BACKUP PLATFORM CONNECTION**

These actions are not required if your alternative restore target is a *managed virtual server (dedicated)* – we’ll do this for you.

If your alternative restore target is a *virtual server (shared) or virtual server (dedicated)*, use this process to either:

- Temporarily redirect a restore target virtual server to a different backup platform
- Switch a restore target virtual server back to its original backup platform

If you’re required to perform the redirect for the restore, we’ll send you an email with the new platform address you need to temporarily connect to.

*Do not* switch your target virtual server back to its original platform, until we advise you by email the restore has been completed.

The method for connecting a virtual server to a backup platform varies according to your virtual server’s operating system.

**CHANGING A BACKUP PLATFORM CONNECTION FOR A VIRTUAL SERVER RUNNING WINDOWS**

Right click the *Avamar* icon in your task tray.

Select *Manage*, then select *Activate Client*. 
The Activate Client Setup window will appear.

The Administrator Server Address field will be pre-populated with the address of your virtual server’s current backup platform. This example shows a connection to stlava03un01.tsb.avamar.com.au.

If you just want to check the backup platform your virtual server is connected to, you can select Close at this stage to leave the settings unchanged.

If you are changing the backup platform, take note of the existing platform address before you redirect. The name of a virtual server’s current backup platform (Administrator server) appears in your most recent daily backup report.

Highlight the Administrator Server Address field, and replace the entry with the address of either:

- The backup platform where your backup file(s) is stored (before starting the redirected restore)
- The original backup platform of your target virtual server (once we advise you the restore is complete)

The pre-populated Client Domain will be replaced with ‘/’.
If you’re restoring from a short-term backup, then you’ll need to enter your details in the Client Domain field. Refer to your most recent daily backup report for this information.

If you are restoring from a long-term backup, leave the Client Domain field as ‘/’.

Select Activate.

The following message will be displayed only if your target virtual server has previously been configured for scheduled backups.

Select Yes.

A message should appear to confirm connection to a different backup platform was successful.

Select OK to complete the process.

**CHANGING A BACKUP PLATFORM CONNECTION FOR A VIRTUAL SERVER RUNNING LINUX**

Find which backup platform your restore target virtual server is connected to by entering the following command:

```
root@lxtsbres01:~# service avagent status
```
In this example, the following response shows that the virtual server is currently connected to the backup platform address: tsbava12un01.tsb.avamar.com.au

avagent Info: Client Agent is running.
avagent Info: Client activated with MCS "tsbava12un01:28001"
avagent Info: Client using DPN "tsbava12un01.tsb.avamar.com.au"
avagent Info: avagent script version 11
  version: 6.0.101-66
  build date: Nov 5 2011 13:13:04
  msg format: 13-10
  SSL: TLSv1 OpenSSL 0.9.8g 19 Oct 2007
  Zlib: 1.2.1.2
  LZO: 1.08 Jul 12 2002
  platform: Linux
  OS version: RHEL
  Processor: i686

If you are changing the backup platform, take note of the existing platform address before you redirect. The name of a virtual server’s current backup platform (Administrator server) appears in your most recent daily backup report.

To connect to a different backup platform, enter the command:

```
root@lxtsbres01:~#/usr/local/avamar/bin/avregister
```

This script will register and activate the client with the Administrator server.

Then enter either:
- The backup platform where your backup file(s) is stored (before starting the redirected restore)
- The original backup platform of your target virtual server (once we advise you the restore is complete)

Enter the address of the new backup platform in the format: (DNS text name or numeric IP address, DNS name preferred).

Enter the Client Domain field.

If you’re restoring from a short-term backup, then you’ll need to enter your details in the Client Domain field. Refer to your most recent daily backup report in the Domain Name column.

If you’re restoring from a long-term backup, leave the Client Domain field blank and press the enter key.

Enter the Avamar server domain [clients]:

In the following example, the new backup platform being connected to is tsbava11un01.

```
root@lxtsbres01:~#/usr/local/avamar/bin/avregister
```

This script will register and activate the client with the Administrator server.

Enter the Administrator server address (DNS text name or numeric IP address, DNS name preferred): tsbava11un01

Enter the Avamar server domain [clients]:

avagent.d Info: Stopping Avamar client Agent (avagent)...
avagent.d Info: Client Agent stopped.
avagent Info <5241>: Logging to /usr/local/avamar/var/avagent.log
avagent.d Info: Client activated successfully.
avagent Info <5241>: Logging to /usr/local/avamar/var/avagent.log
avagent Info <5417>: daemonized as process id 22187
avagent.d Info: Client Agent started.
Registration Complete.

The command is only successful if Registration Complete displays.
If you only have Linux servers, you won’t have the backup administrator, which means you’ll need to use command lines to list all backups on a server and to initiate non-scheduled backups and restores.

In these examples:

- `cllxprmgtlog01.ncs.corp.telstra.com` is the server
- `maradmin` is the backup user name
- `PSL_Infrastructure` is the top level domain name

**LIST ALL BACKUPS ON A SERVER**

```
avtar --backups --id=maradmin@/PSL_Infrastructure --account=/PSL_Infrastructure/pslclastd003/cllxprmgtlog01.ncs.corp.telstra.com
```

**RESTORE TO A BACKUP**

In this example, the file `/etc/hosts` is restored to a target of `testrestore` on the server:

```
cllxprmgtlog01.ncs.corp.telstra.com
avtar -xv --target="/testrestore/" /etc/hosts --id=maradmin@/PSL_Infrastructure --account=/PSL_Infrastructure/pslclastd003/cllxprmgtlog01.ncs.corp.telstra.com
```

**BACKUP**

To back up a file called `/etc/hosts` on the server, for this example enter:

```
cllxprmgtlog01.ncs.corp.telstra.com
avtar -cv /etc/hosts --id=maradmin@/PSL_Infrastructure --account=/PSL_Infrastructure/pslclastd003/cllxprmgtlog01.ncs.corp.telstra.com
```