Technical Guide

How to Use DAIR Cloud Resources: Linux/Windows/GPU
# Table of Contents

## Security and Account Defaults
- Using SSH Keys to Secure Access to Your VMs
- Setup Security Groups / Firewalls
- Creating Default Accounts for Your VMs

## The Basics
- Creating an Instance or Virtual Machine (VM)
- Logging into an Instance
- GPU Specific Access over VNC
- Creating User Accounts

## Advanced Topics (Linux OS instances only)
- Morpheus CLI
Security and Account Defaults:
Creating and Using Your SSH Key
(SSH key logins are required in DAIR)
Web Login to the DAIR Cloud:

> https://cloud.canarie.ca/login/auth

> Use credentials emailed to you
Adding your SSH key to DAIR

Instructions for creating a key follow.

Return to this page to add your key once created.
How to Create an SSH Key (Mac or Linux)

1. On MacOS
   • Open a terminal and go to Step 3

2. On Windows 10
   • Add the Linux subsystem for windows
     (see https://docs.microsoft.com/en-us/windows/wsl/install-win10)
   • Install Ubuntu or CentOS from the app store
   • Open Linux command shell window from Start menu

3. On the command prompt run this command:
   $ ssh-keygen -t rsa -m PEM -C "your email address"
   • Follow the directions and name your Key something memorable
   • Add a passphrase if you want a more secure key, just don’t forget it!

4. This will create 2 files; “Name”(private key) and “name.pub”(public key)

5. Run the “cat” command on each file so you can copy and paste keys into your key-pair fields (Step 3 on previous slide)
How to Create an SSH Key (Win-8.x or earlier)

> Download “Putty” tool, the MSI complete installer, or:
> Download putty.exe and puttygen.exe


---

### Alternative binary files

The installer packages above will provide versions of all of these (except PuTTYtel), but you can download standalone binary files. (Not sure whether you want the 32-bit or the 64-bit version? Read the FAQ entry.)

<table>
<thead>
<tr>
<th>Package</th>
<th>Bit</th>
<th>File</th>
<th>Download</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>putty.exe (the SSH and Telnet client itself)</td>
<td>32-bit</td>
<td>putty.exe</td>
<td>(or by FTP)</td>
<td>(signature)</td>
</tr>
<tr>
<td>64-bit</td>
<td>putty.exe</td>
<td>(or by FTP)</td>
<td>(signature)</td>
<td></td>
</tr>
<tr>
<td>pscp.exe (an SCP client, i.e. command-line secure file copy)</td>
<td>32-bit</td>
<td>pscp.exe</td>
<td>(or by FTP)</td>
<td>(signature)</td>
</tr>
<tr>
<td>64-bit</td>
<td>pscp.exe</td>
<td>(or by FTP)</td>
<td>(signature)</td>
<td></td>
</tr>
<tr>
<td>puttytel.exe (a Telnet-only client)</td>
<td>32-bit</td>
<td>puttytel.exe</td>
<td>(or by FTP)</td>
<td>(signature)</td>
</tr>
<tr>
<td>64-bit</td>
<td>puttytel.exe</td>
<td>(or by FTP)</td>
<td>(signature)</td>
<td></td>
</tr>
<tr>
<td>plink.exe (a command-line interface to the PuTTY back ends)</td>
<td>32-bit</td>
<td>plink.exe</td>
<td>(or by FTP)</td>
<td>(signature)</td>
</tr>
<tr>
<td>64-bit</td>
<td>plink.exe</td>
<td>(or by FTP)</td>
<td>(signature)</td>
<td></td>
</tr>
<tr>
<td>pagesant.exe (an SSH authentication agent for PuTTY, PSCP, PSFTP, and Plink)</td>
<td>32-bit</td>
<td>pagesant.exe</td>
<td>(or by FTP)</td>
<td>(signature)</td>
</tr>
<tr>
<td>64-bit</td>
<td>pagesant.exe</td>
<td>(or by FTP)</td>
<td>(signature)</td>
<td></td>
</tr>
<tr>
<td>puttygen.exe (a RSA and DSA key generation utility)</td>
<td>32-bit</td>
<td>puttygen.exe</td>
<td>(or by FTP)</td>
<td>(signature)</td>
</tr>
<tr>
<td>64-bit</td>
<td>puttygen.exe</td>
<td>(or by FTP)</td>
<td>(signature)</td>
<td></td>
</tr>
</tbody>
</table>
Create an SSH Key with Puttygen (Cont’d)

On Windows 8.1 and earlier versions:

> Start Puttygen – Generate and copy public key

1. Start Puttygen and select “Generate” to generate a new key.
2. A window will appear showing the public key. Click “Copy” to copy it to the clipboard.
3. Paste the public key into Morpheus.
Create an SSH Key with Puttygen (Cont’d)

> Export your private key...

> Copy private key and paste in Morpheus (see Slide 5)
Create an SSH Key with Puttygen (Cont’d)

> Save your Private Key on your local Windows machine for use in Putty.

Once complete, return to page 5 for instructions on entering your key.
Security and Account Defaults: Setup Security Groups / Firewalls
Avoid Getting Hacked!

> Security group rules for SSH connections **must not have a CIDR of 0.0.0.0/0**
  
  • The CIDR value specifies the allowable source IP address range for computers connecting to an instance
  • All-zeros allows any computer in the world access and makes your instance highly vulnerable to attacks

> You must know the public IP address of the computer(s) you would like to permit access to your VMs in DAIR
  
  • You can determine your IP by searching Google for “what is my IP” on each machine you want to give access to
  • For example, to enable only a single IP address, make the CIDR aa.bb.cc.dd/32 (where aa.bb.cc.dd is your public IP numeric value)

> Create a new rule for each IP address that you wish to grant SSH access (see details on next slide)
Configure/Edit your Firewall Rules

A. Instance Count

B. Instance Status

C. Default Rules

1. Select All
2. NETWORK
3. SECURITY GROUPS
4. ADD RULE

Click to go to Instance View

Allows your Instances to talk to the internet

22 & 5901 Allows Console to work
443 & 80 is for agent updates
To Add a Firewall Rule

- Name your Rule
  - Name: Tenant SSH Access

- Range ##
  - Direction: ingress
  - Rule Type: Custom Rule
  - Protocol: TCP
  - Port Range: 22

- Other Options
  - Source Type: network
  - Source: 242.334.123.23/32
  - Destination Type: instance

- /32 after IP allows only source IP access (not a range of IPs)

Save Changes
Security and Account Defaults: Creating Default Accounts for Your VMs
Configure Your Tenant Account
This must be done before deploying an instance

Set default user ID, password and SSH key which will be used for any new Linux instance you create under your account.

Create a user ID and password on any new Windows instance created.
Configure Your Tenant Account for successful Provisioning

1. Navigate to the Provisioning section.
2. Set Administrator Password for Windows here.
3. Click SAVE.
The Basics:
Creating an Instance or Virtual Machine (VM)
Creating your First Instance

1. Navigate to the Provisioning section.
2. Select the Instances option.
3. Add a new instance.
Creating an Instance: Platform and Cloud

New instances may be provisioned based on OS type.

Choose your Platform

Choose your Group

1. CENTOS
   A popular Linux flavor operating system. Easily provision CentOS vms for various engines including Docker.

2. DEBIAN

3. DOCKER
   An open platform for distributed applications for developers and sysadmins. Deploy any container from any docker registry.

4. UBUNTU
   Ubuntu images

5. WINDOWS
   Windows Server
GPU Specific Details

![CREATE INSTANCE](image)

**Select OS Versions**

- You will see resources with your tenant name for these

**Select if you want an Public IP (Internet)**

- Always set Volumes to Local!
Creating a Windows Instance:
Provision configuration options for your instance.

Select OS Versions
Select Plan Notice: price changes:
You will see resources with your tenant name for these
Select if you want an Public IP (Internet)
Create security rules to open ports for your instance.

For Azure you can create or select an availability set for an instance
Creating a Windows Instance:

Some advanced configuration options:

- Deployment
- Scale
- Backups
- Lifecycle

> Review and Complete
Creating a Windows Instance:

**INSTANCE COUNT**

- Running: 0
- Stopped: 1

**INSTANCE STATUS**

- MAX CPU: 0%
- STORAGE: 0%
- MEMORY: 0%

**INSTANCES**

- WINTest1: Version: 2016
  - Virtual Machines: 1
  - Group: AWS-Canada
  - Clouds: AWS-Canada

**Click to go to Instance View**
Creating a Windows Instance:

RDP to this IP using Microsoft Remote Desktop Using the admin password or the user account you setup.

If you are prompted for a login in the console tab, you have not properly provisioned your account settings. See Pages 16-17.
Creating a Linux Instance:

> Provision configuration options for your instance.

Select OS Versions
Select Plan
Notice: price changes:
You will see resources with your tenant name for these
Select if you want an Public IP (Internet)
Create security rules to open ports for your instance.

For Azure you can create or select an availability set for an instance.
Creating a Linux Instance:

Some advanced configuration options:

- Deployment
- Scale
- Backups
- Lifecycle

> Review and Complete

**Summary**

**INSTANCE OPTIONS**

- NAME: TESTinstance1
- GROUP: AWS-Canada
- CLOUD: AWS-Canada
- TYPE: UBUNTU
- PLAN: Amazon TZ Medium - 2 Core, 4GB Memory
- VERSION: 16.04
- LAYOUT: Ubuntu
- PRICE: CAD50.1711 / Month

**VOLUMES**

- root: 40 GB gp2

**NETWORKS**

- DMAR-TEST: TENANT-a21 (subnet-05ab76cf980d8e91a) : DHCP
Creating a Linux Instance:

- Running: 3 instances
- Stopped: 1 instance

INSTANCE COUNT

INSTANCE STATUS

INSTANCES

- TESTInstance1
  - SSH: 10.1.19.5.22
  - Version: 16.04
  - Group: AWS-Canada
  - Clouds: AWS-Canada

Click to go to Instance View
Creating a Linux Instance:

### TESTInstance1

Plan: Amazon T2 Medium - 2 Core, 4GB Memory

<table>
<thead>
<tr>
<th>STATUS</th>
<th>HEALTH</th>
<th>LAST BACKUP</th>
<th>AVAILABILITY</th>
<th>OMS</th>
<th>MAX CPU</th>
<th>MEMORY</th>
<th>STORAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>100.000%</td>
<td></td>
<td>0%</td>
<td>7%</td>
<td>4%</td>
</tr>
</tbody>
</table>

**INFO**

- **Group:** AWS-Canada
- **Created By:** TEST THETESTER
- **Cores:** 2
- **Price:** CAD50.1711 / Month

Cloud: AWS-Canada
- **Layout:** Ubuntu
- **Memory:** 4.0GiB
- **Source Image:** Morphbox Ubuntu 16.04.3

**Date Created:** 06/05/2019 02:45 PM
- **Version:** 16.04
- **Total Storage:** 40.0GiB
- **Provision Time:** 2 minutes 23 seconds

**VMS**

<table>
<thead>
<tr>
<th>STATUS</th>
<th>NAME</th>
<th>TYPE</th>
<th>CLOUD</th>
<th>LOCATION</th>
<th>COMPUTE</th>
<th>MEMORY</th>
<th>STORAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>TESTInstance1</td>
<td>Ubuntu 16.04</td>
<td>AWS-Canada</td>
<td>35.183.53.22</td>
<td>6</td>
<td>4</td>
<td>0</td>
</tr>
</tbody>
</table>

### Summary

<table>
<thead>
<tr>
<th>NAME</th>
<th>DESCRIPTION</th>
<th>CREATED BY</th>
<th>START DATE</th>
<th>ETA/DURATION</th>
<th>STATUS</th>
<th>ERROR</th>
</tr>
</thead>
<tbody>
<tr>
<td>TESTInstance1</td>
<td>Provision</td>
<td>TEST THETESTER</td>
<td>06/05/2019 02:45 PM</td>
<td>00:02:22</td>
<td>Complete</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Prepare Resources</td>
<td></td>
<td>06/05/2019 02:45 PM</td>
<td>00:00:33</td>
<td>Complete</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Finalize</td>
<td></td>
<td>06/05/2019 02:45 PM</td>
<td>00:01:49</td>
<td>Complete</td>
<td></td>
</tr>
</tbody>
</table>

Login to instance
The Basics: Logging into an Instance
Login to Your Linux Instance – Option 1

> Use the built-in console (web browser)
> You are auto logged in with the account you setup

If you are prompted for a login in the console tab, you have not properly provisioned your account settings. See Pages 16-17.
Login to Your Linux Instance – Option 2

> Use your SSH client application

> Mac & Windows (with Linux subsystem)

```bash
ssh -i /path/to/your/key/yourkey username@XXX.XXX.XXX.XXX
```

> Your IP is listed under “Location”
Login to Your Linux Instance – Option 3

On your Windows machine:

> Locate and run putty.exe (previously installed, see Slide-7)

> Use the IP (see previous slide) and Username you defined in your Morpheus default user settings (see Slide-16) to create a new “putty” session as shown in the following slides.
Login to Your Linux Instance – Option 3
Login to Your Linux Instance – Option 3

1. Select the Session category.
2. Navigate to Saved Sessions.
3. Click on Save.
4. Click on Open.
Login to Your Linux Instance – Option 3

> Click “Session”
> Enter a “Saved Session” name
> Click “Save”
> Finally “Open” to start an SSH session to your server
The Basics:
Secure VNC to XWindows for Linux GPU Based Instances
Login: VNC to XWindows (MAC or Linux)

> Setup an SSH tunnel to your instance

https://github.com/apenwarr/sshuttle

> OSX process
  > Change uname to your username

```
ssh -i ~/yourkey -p 22 uname@208.75.7x.xxx -L 5901:127.0.0.1:5901 sleep 2h
```

> This terminal will be unusable until you terminate the tunnel
Login: VNC to XWindows (MAC or Linux)

> Use the username and password you set up in the Morpheus account setup

> Install TurboVNC

> Run TurboVNC viewer

> Connect as illustrated

```
ssh-I /{downloadsDirectory}/{Keypair}.pem
Ubuntu@208.75.7x.yy
```

```
sudo passwd ubuntu
New Password:
Re-enter New Password:
```

https://sourceforge.net/projects/turbovnc/files/
Login: VNC to XWindows (MAC or Linux)

> Login to XWindows
> Enter username and the password you just setup for Ubuntu or CentOS
> You are logged into XWindows
> Select use default config
> You now have access to XWindows and can run GPU GUI applications
Login: VNC to XWindows (Windows)

> Locate and run putty.exe
  > See Slide-7 if putty is not installed
> Load your previous saved Putty session
> Edit Hostname to match your IP
Login: VNC to XWindows (Windows)

> Click “SSH”
> Enable compression
> Set SSH Protocol Version to “2”
Login: VNC to XWindows (Windows)

> Open “SSH”
> Click “Tunnels”
> Set up new forwarding port as seen here
> Click “Add”
Login: VNC to XWindows (Windows)

- Click “Session”
- Enter a “Saved Session” name
- Click “Save”
- Finally, “Open” to start SSH session with an established tunnel for Secure VNC access
Login: VNC to XWindows (Windows)

> From the putty terminal
> Add password to ubuntu user
  > For CentOS, use “CentOS” instead of “Ubuntu”
> Install TurboVNC
> Run TurboVNC viewer
> Connect as illustrated

sudo passwd ubuntu
New Password:
Re-enter New Password:

Turbo VNC download location:
https://sourceforge.net/projects/turbovnc/files/
Login: VNC to XWindows (Windows)

> Login to XWindows
> Enter username and the password you just setup for Ubuntu or CentOS
> You are logged into XWindows.
> Select “Use default config”
> You now have access to XWindows and can run GPU GUI applications.
The Basics: Creating User Accounts
Create a User Account on Your Linux VM

Connect to your Linux instance using SSH:

Use the adduser command to add a new user account to an EC2 instance (replace new_user with the new account name). The following example creates an associated group, home directory, and an entry in the /etc/passwd file of the instance:

```
$ sudo adduser new_user
```

Note: If you add the new_user to an Ubuntu instance, include the `—disabled-password` option to avoid adding a password to the new account:

```
$ sudo adduser --disabled-password new_user
```

Change the security context to the new_user account so that folders and files you create will have the correct permissions:

```
$ sudo su - new_user
```

Note: When you run the `sudo su - new_user` command, the name at the top of the command shell prompt changes to reflect the new user account context of your shell session.

Create a .ssh directory in the new_user home directory:

```
$ mkdir .ssh
```

Use the `chmod` command to change the .ssh directory’s permissions to 700. Changing the permissions restricts access so that only the new_user can read, write, or open the .ssh directory.

```
$ chmod 700 .ssh
```

Use the `touch` command to create the authorized_keys file in the .ssh directory:

```
$ touch .ssh/authorized_keys
```

Use the `chmod` command to change the .ssh/authorized_keys file permissions to 600. Changing the file permissions restricts read or write access to the new_user.

```
$ chmod 600 .ssh/authorized_keys
```

open their public key in a text editor and edit with vi or other Linux text edit and insert the private key then save the file.

```
$ vi .ssh/authorized_keys
```
Advanced Topics: Morpheus Command Line
Using Morpheus CLI Commands

> Anything you perform through the Dashboard may be performed through CLI commands or the Morpheus API.

> Documentation can be found here:

  - CLI:

  - API: