Troubleshooting

Virtual Desktop Service

NetApp
September 12, 2021

Table of Contents

Troubleshooting

Troubleshooting Failed VDS Actions

Overview

Much of the logging that happens in VDS is not exposed in the web UI due to the sheer volume of it. More detailed logs are found on the end point. These logs are described below.

In VDS v5.4+, the logs are found in the following folder path:

```
C:\programdata\cloudworkspace
```

In previous version of VDS, they can reside in the following paths:

```
C:\Program Files\CloudWorkspace\
C:\Program Files\CloudJumper\
C:\Program Files\IndependenceIT\
```

File type also varies by VDS version, log files are either .txt or .log files found in sub-folders of the above outlined path.

Automation logs

CW VM Automation Service log

```
CwVmAutomationService.log
```

The CW VM Automation service is a Windows Service that is responsible for the management of all Virtual Machines in the deployment. As a Windows Service it is always running in a deployment, but has two main modes of operation: Scheduled Task Mode and Event Mode.

Scheduled Task Mode consists of activities that are performed on the VMs as part of a schedule, including collection sizing and performance data, rebooting VMs, checking on state (on or off) vs rule sets generated by the Workload Schedule and Live Scaling features. The logs denote these action types in the 5th column with names like “Daily Actions”, “Weekly Actions” and “Daily Maintenance”. If you are troubleshooting questions like “Why did Server X reboot last night at 2:00 am” or “Why is this server on when I think it should be off” then the scheduled tasks for those specific VMs are usually the best place to look.

Event Mode is activated when a user or other VDS Service such as the CW Automation Service asks for a Task to be completed. Examples of this type of activity include a user request to Create a new Server or CW Automation requesting the sizing and state of servers to be checked because more users were added to the workspace. These events typically have log entries with both the event name “Create Server” and the actual name of the VM right next to it (ex: Create Server NNXTS2). When troubleshooting these types of events, its usually best to scroll to the bottom of the log and then to an upwards search for the VM name. You can then scroll up more rows to see where the process started.

CW Automation Service log

```
CWAutomationService.log
```

The CW Automation Service log is the primary Windows services for managing the components of a Workspace deployment. It runs the tasks required to manage users, applications, data devices, and policy. In addition, it can create tasks for the CW VM Automation Service when changes need to be made to size, count, or state of the VMs in the deployment.

Like the CW VM Automation Service, the CW Automation service executes both scheduled tasks and event driven tasks, with the latter being the more frequent type. The log for the CW Automation Service starts each line with the entity and action being worked on (ex: Start Server NNXTS1) so searching for the entity name from the bottom of the file is the quickest way to find the specific log lines that apply to the task.

CW Agent Service log

```
CwAgent.log
```

The CW Agent Service performs all the tasks that are local to a specific VM, including checking the resource levels and utilization for the VM, checking that the VM has a valid certificate for TLS traffic, and checking to see if the mandatory reboot period has been reached. Besides checking on detail information on these tasks, this log can also be used to check for unexpected VM restarts or unexpected network or resource activity.

CWManagerX log

```
CWManagerX.log
```

CWManagerX is a web service that provides the communication link between the local Deployment and the VDS global control plane. Tasks and data requests that originate in the VDS Web Application or VDS API are communicated to the local deployment through this web service. From there, the tasks and requests are directed to the appropriate web service (described above) or in rare cases directly to Active Directory. Since this is mostly a communications link there isn't much logging that occurs during normal communication, but this log will contain errors when the communication link is broken or performing incorrectly.

DC Config log

```
DCConfig.log
```

DC Config is a Windows application that provides Deployment specific configuration parameters that are not exposed in the VDS Web Application interface. The DC Config log details the activities runs when configuration changes are made in DC Config.

CAVDCDeployment log

```
CAVDCDeployment.log
```

CW vDC Deployment is a Windows application that performs the tasks necessary to create a Deployment in Azure. The log tracks the configuration of the Cloud Workspace windows services, default GPOs, and routing and resource rules.

Miscellaneous logs

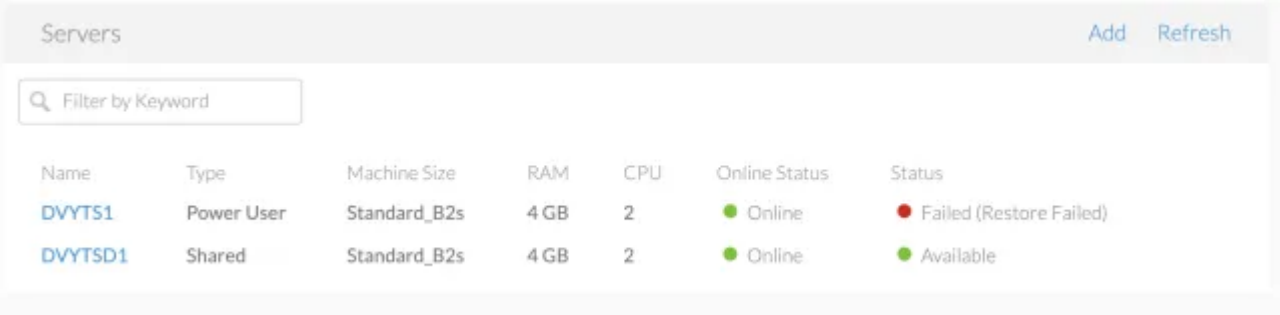
```
CwVmAutomationService-Installing.log
CwAgent-Installing.log
```

The remaining logs track the installation of the Windows Services and application described above. Since VDS services auto-update when a new version is targeted at that specific deployment, these logs track the upgrade process since the Service or application typically needs to be off while being upgraded. If you find the Services are consistently Stopped these logs can help identify if a failed upgrade to a specific service is the cause. In these cases, we would expect to see an error in these logs detailing why the upgrade failed.

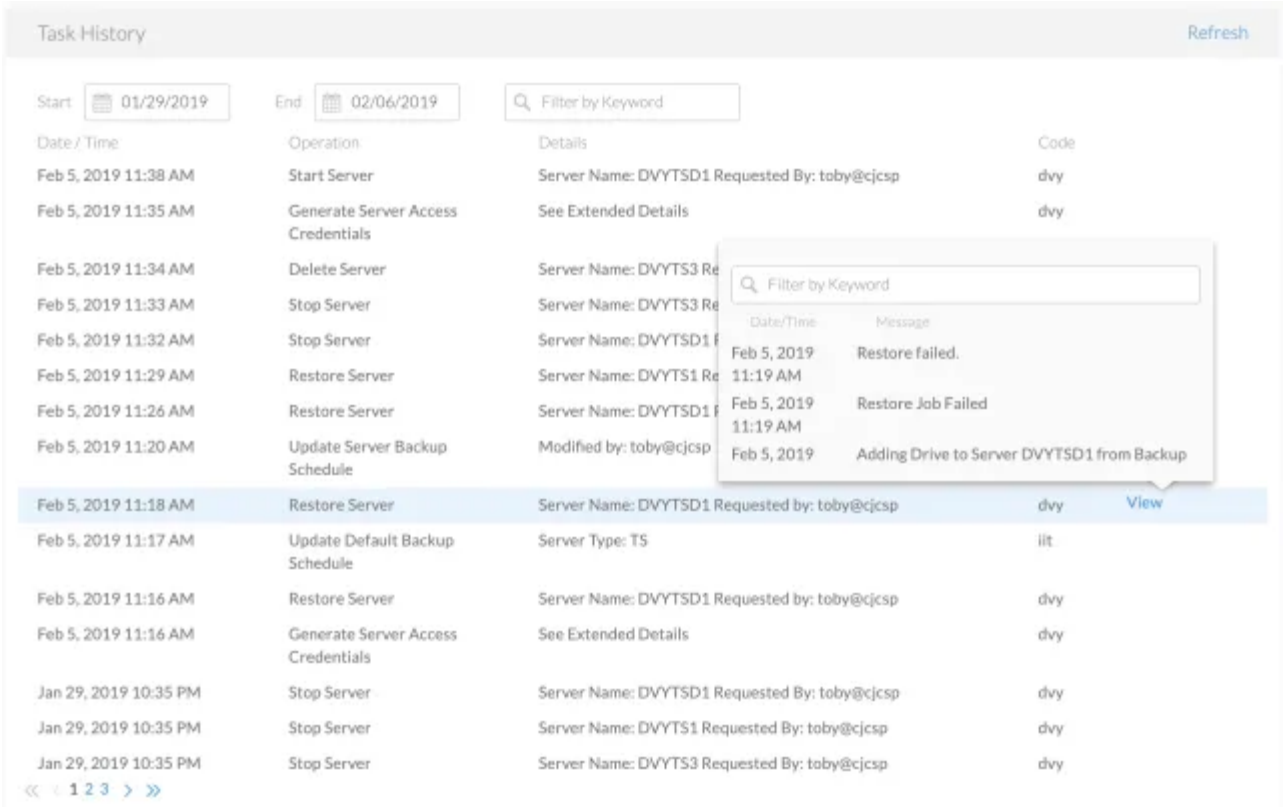
Accessing logs and reviewing information

When requested actions like cloning a server, adding a user or restoring a backup you'll get feedback in the VDS UI.

+

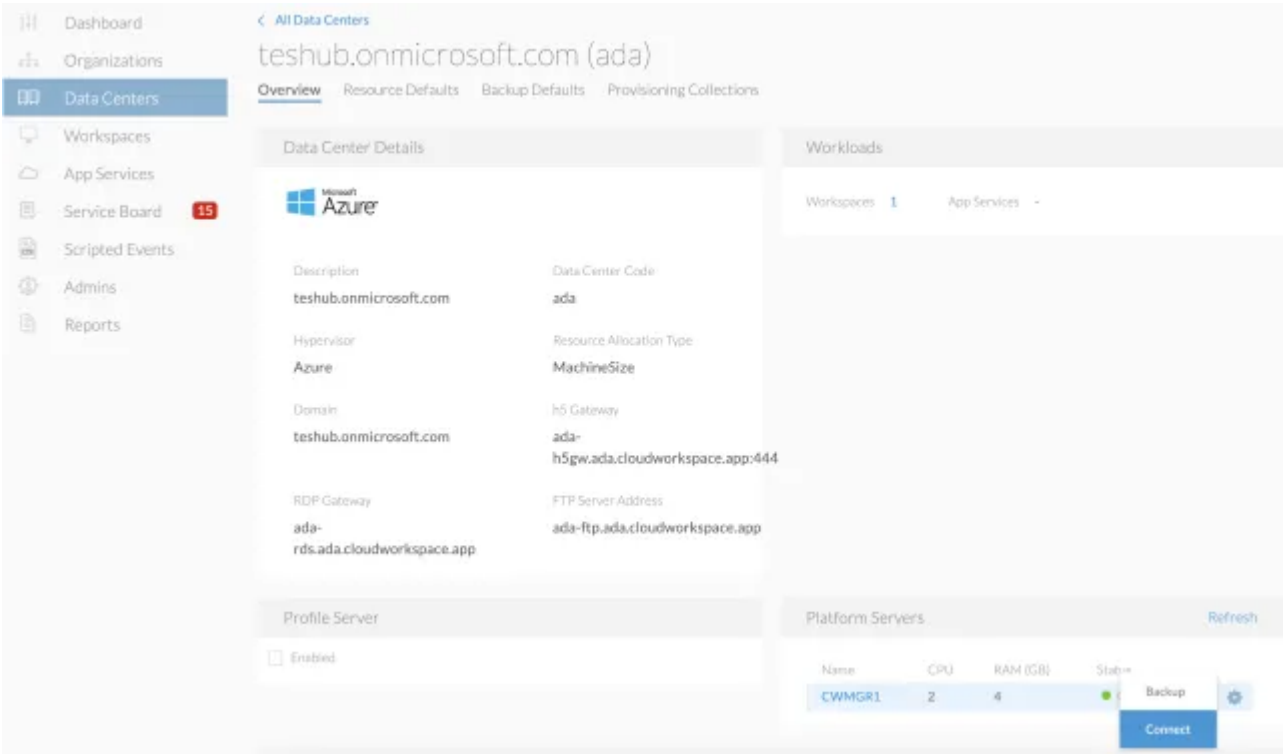


1. VDS keeps detailed logs and exposes some of them on the Task History section of the Deployments page in VDS. Click on View can show details of the listed tasks.



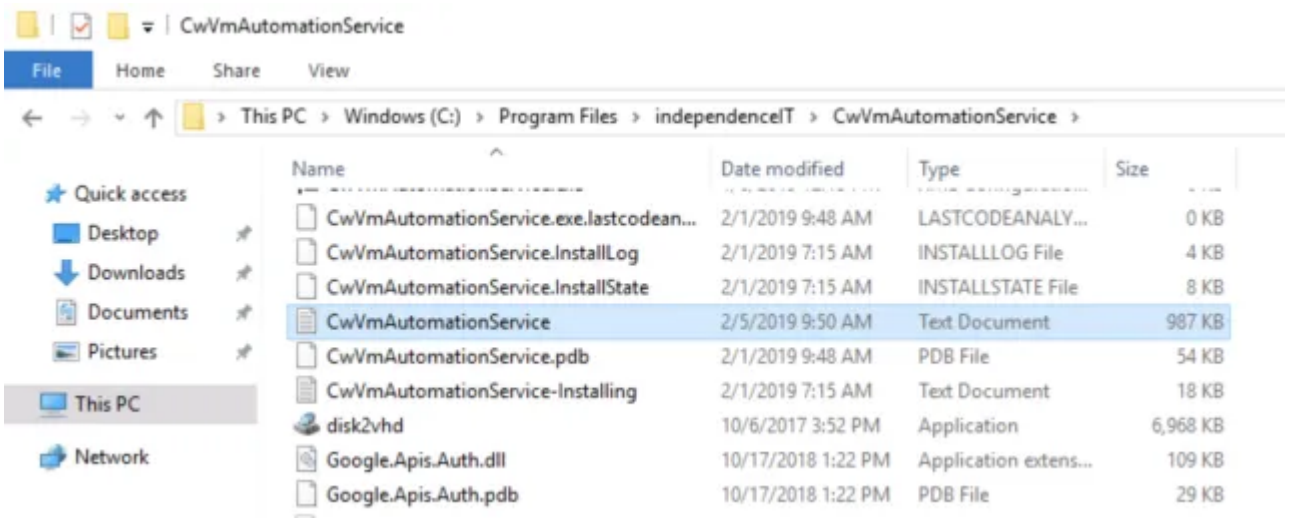
2. Sometimes the Task History does not contain enough details to identify the true root cause. In order to keep the Task History section usable and not overwhelmed by all logged events, only a subset of task information is presented here. For a deeper look the text log files referenced above can provide more details.

   a. To access this log, navigate to the Deployments Section and click the Gear Icon next to the CWMGR1 VM, then click Connect (or in the case of the CwAgent log, connect to the appropriate VM)

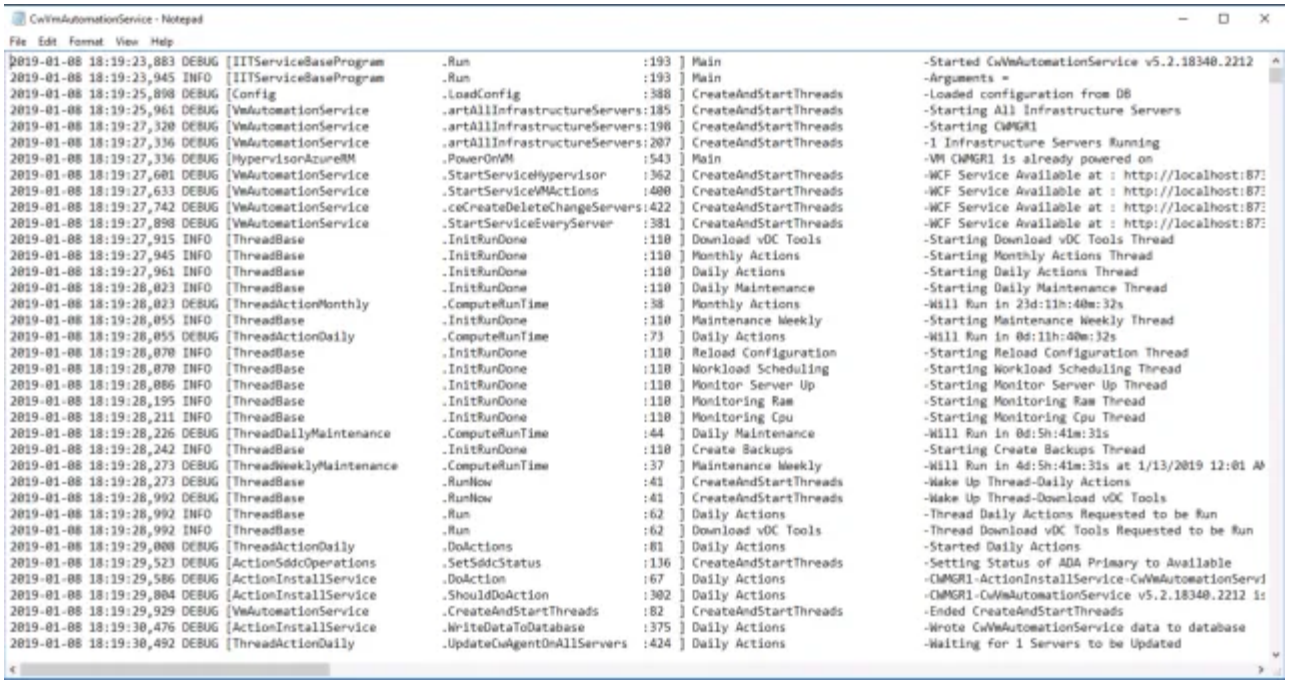


3. When connecting to a Platform Sever (Like the CWMGR1) you will not be automatically logged into the server (unlike connecting to a server in the tenant). You'll need to login with a Level3 .tech account.

4. Then navigate to the path as shown above and open the log file.



5. This text file contains a log of all events, listed form oldest to newest:



6. When opening a support case with NetApp VDS, being able to provide the errors found here will SIGNIFICANTLY accelerate the speed to resolution.

Internet Connection Quality Troubleshooting

Symptoms

Dropped users connections requiring a reconnect. Laggy interface response, general performance problems that don’t appear to be related to resource (RAM/CPU) loads.

Cause

When users report performance issues, dropped user connections or a laggy interface, the most common cause is not resources at all but rather the network connections between the customer and the datacenter. These connections run through their ISP, various internet backbone carriers and ultimately into the datacenter. Along the way the data traverses multiple stops. Each of theses hops can introduce network latency, lost packets and jitter, all of these can contribute to the perceived performance of the desktop computing environment in the virtual desktop.

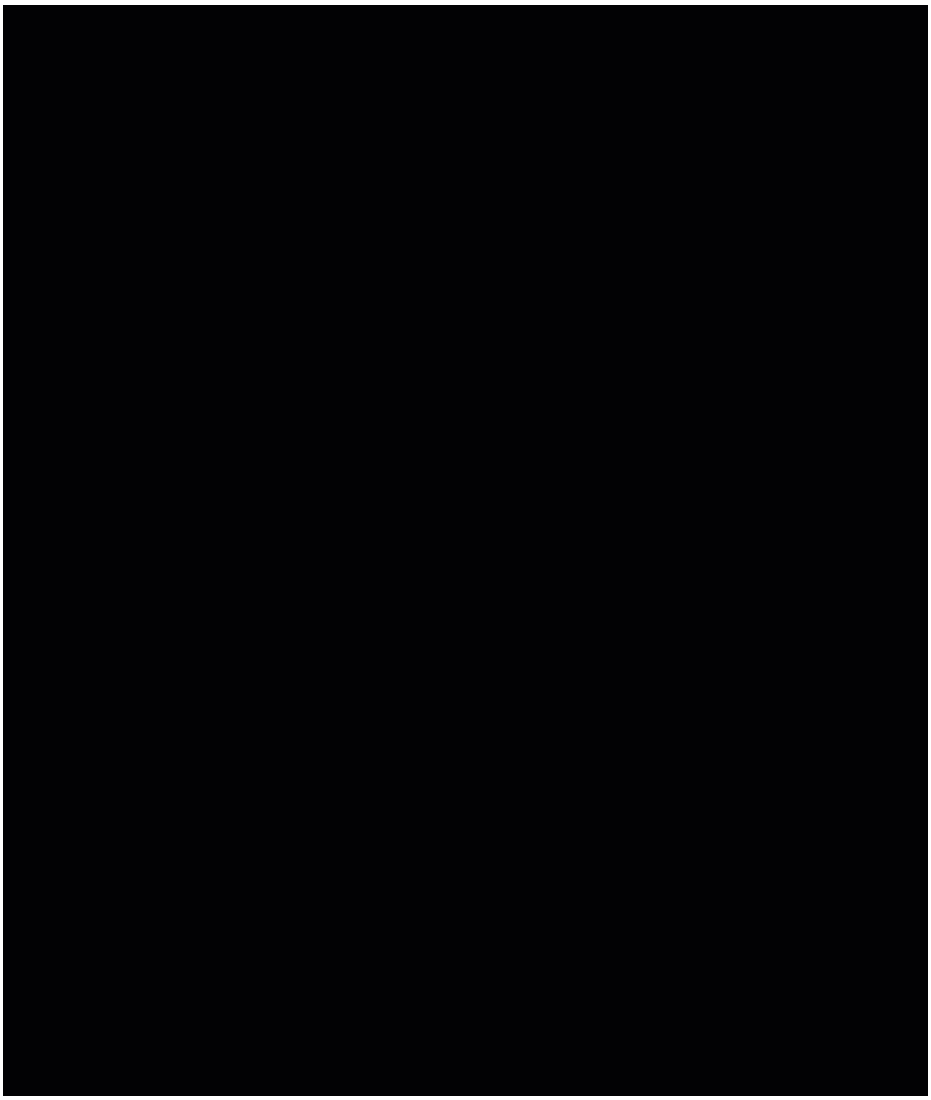
Tier 1 triage and troubleshooting will include basic steps like confirming resources (RAM, CPU and HDD Space) are sufficient but once that is completed, testing the network connectivity is a great next step in the troubleshooting process.
Resolution

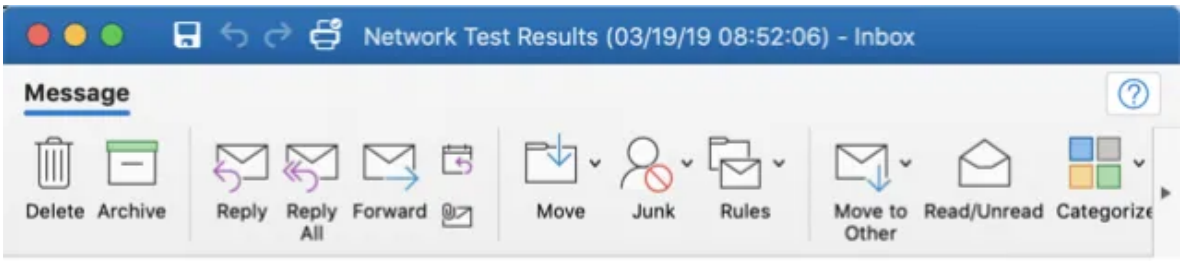
Primary option: NetApp VDS Windows client has built-in diagnostic tools

The diagnostic test can be run and delivered to your email, all from within the virtual desktop Client.

1. Click on the preferences icon (four horizontal lines on the top menu bar)
2. Click Help
3. Click Network Test

4. Enter the user name experiencing the issues, click Run
5. Once complete, enter your email address to receive an email report
6. Review the report to troubleshoot potential connection issues





Network Test Results (03/19/19 08:52:06)

cloudworkspaceclient
Toby vanRoojen
Tuesday, March 19, 2019 at 8:52 AM
Show Details

```
Network Test Results:
API address resolved successfully
API is reachable
Username: toby.vanroojen@cloudjumper.com
Gateway: fcf-rds.fcf.cloudworkspace.app
Tenant: rjb5.fcf.cloudworkspace.app
Gateway resolved to: 13.82.216.254
Gateway is reachable
fcf-rds.fcf.cloudworkspace.app    90.02ms
fcf-rds.fcf.cloudworkspace.app    96.65ms
fcf-rds.fcf.cloudworkspace.app    93.32ms
fcf-rds.fcf.cloudworkspace.app    90.35ms
fcf-rds.fcf.cloudworkspace.app    88.85ms
fcf-rds.fcf.cloudworkspace.app    91.81ms
fcf-rds.fcf.cloudworkspace.app    91.39ms
fcf-rds.fcf.cloudworkspace.app    95.21ms
fcf-rds.fcf.cloudworkspace.app    92.3ms
fcf-rds.fcf.cloudworkspace.app    92.2ms
fcf-rds.fcf.cloudworkspace.app    90.68ms
fcf-rds.fcf.cloudworkspace.app    93.51ms
fcf-rds.fcf.cloudworkspace.app    93.08ms
fcf-rds.fcf.cloudworkspace.app    1019.5ms
fcf-rds.fcf.cloudworkspace.app    90.74ms
fcf-rds.fcf.cloudworkspace.app    3109.41ms
fcf-rds.fcf.cloudworkspace.app    92.28ms
fcf-rds.fcf.cloudworkspace.app    90.4ms
fcf-rds.fcf.cloudworkspace.app    88.61ms
fcf-rds.fcf.cloudworkspace.app    90.88ms
fcf-rds.fcf.cloudworkspace.app    93.46ms
fcf-rds.fcf.cloudworkspace.app    92.99ms
fcf-rds.fcf.cloudworkspace.app    95.7ms
fcf-rds.fcf.cloudworkspace.app    90.11ms
fcf-rds.fcf.cloudworkspace.app    92.49ms
fcf-rds.fcf.cloudworkspace.app    94.54ms
fcf-rds.fcf.cloudworkspace.app    89.77ms
fcf-rds.fcf.cloudworkspace.app    94.84ms
fcf-rds.fcf.cloudworkspace.app    91.9ms
fcf-rds.fcf.cloudworkspace.app    91.62ms
fcf-rds.fcf.cloudworkspace.app    94.07ms
fcf-rds.fcf.cloudworkspace.app    92.1ms
fcf-rds.fcf.cloudworkspace.app    91.91ms
fcf-rds.fcf.cloudworkspace.app    99.07ms
fcf-rds.fcf.cloudworkspace.app    93.89ms
fcf-rds.fcf.cloudworkspace.app    89.78ms
fcf-rds.fcf.cloudworkspace.app    92.65ms
fcf-rds.fcf.cloudworkspace.app    92.26ms
fcf-rds.fcf.cloudworkspace.app    94.82ms
fcf-rds.fcf.cloudworkspace.app    92.64ms
Average Latency: 191.04ms
```

Secondary option: Manual analysis using PingPlotter

To confirm the client's network connection is the culprit you can run the free utility PingPlotter. This utility sends a ping every few seconds and reports on the speed (latency) of the round trip of that ping. It also notes the packet loss (PL) percentage at each hop along the route. When high latency and/or high packet loss is observed it is a good indication that the performance issues are caused by the quality of the internet connection at the hop that is displaying those issues.

1. Download and install Ping Plotter (Available for MacOS, Windows and iOS).
2. Enter the gateway of the data center in which the tenant is deployed.
3. Let it run for several minutes. Ideally while the performance issues or disconnections are being experienced.
4. Capture the data by choosing "Save Image…" from the File Menu if it is needed for additional troubleshooting.

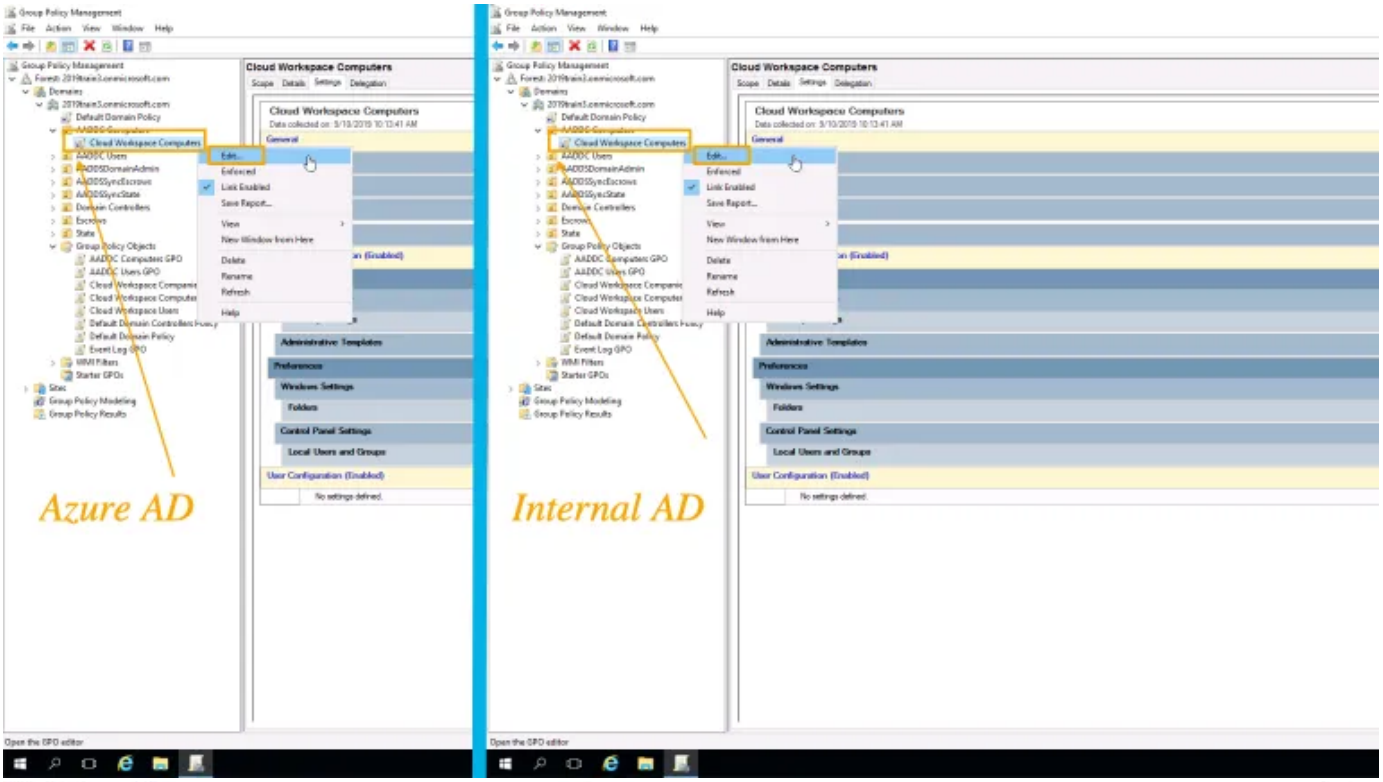
Enable Desktop Wallpaper for User Sessions

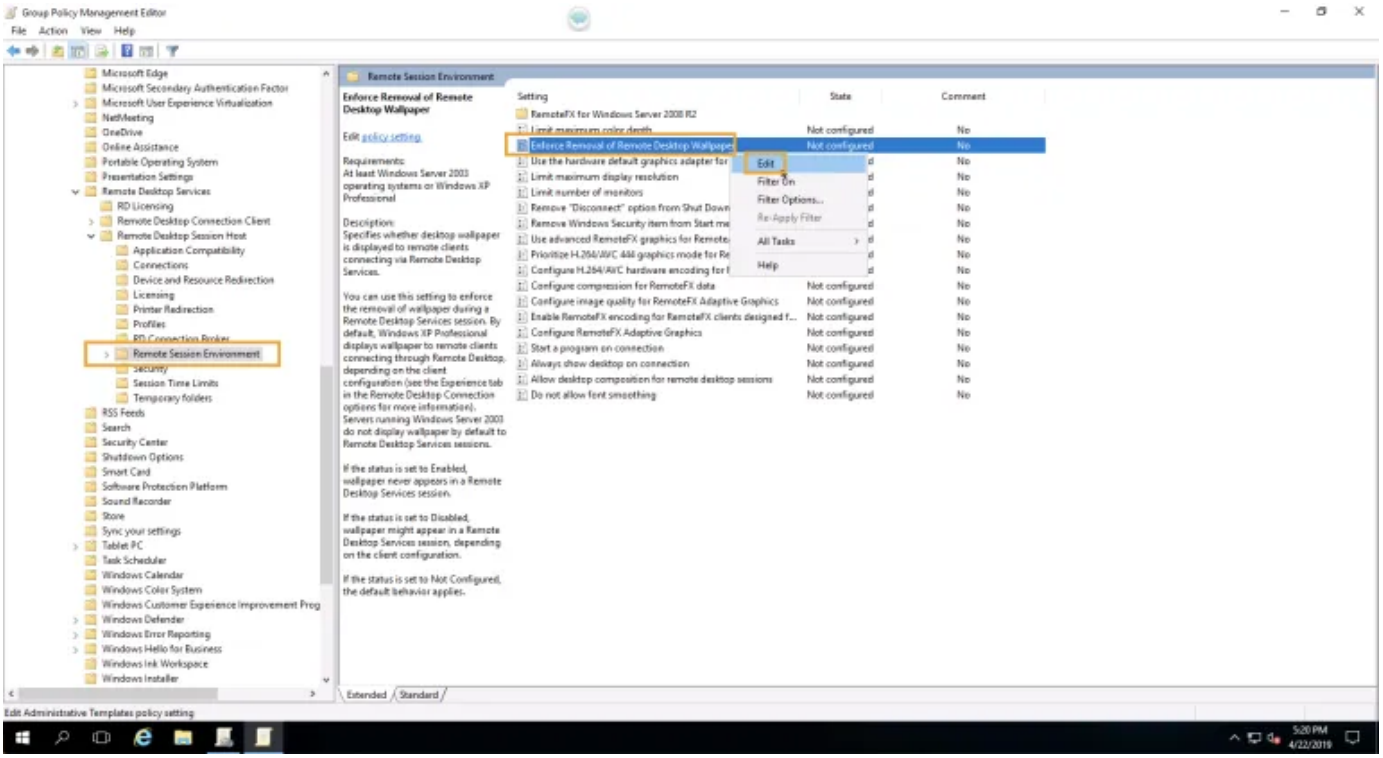
Overview

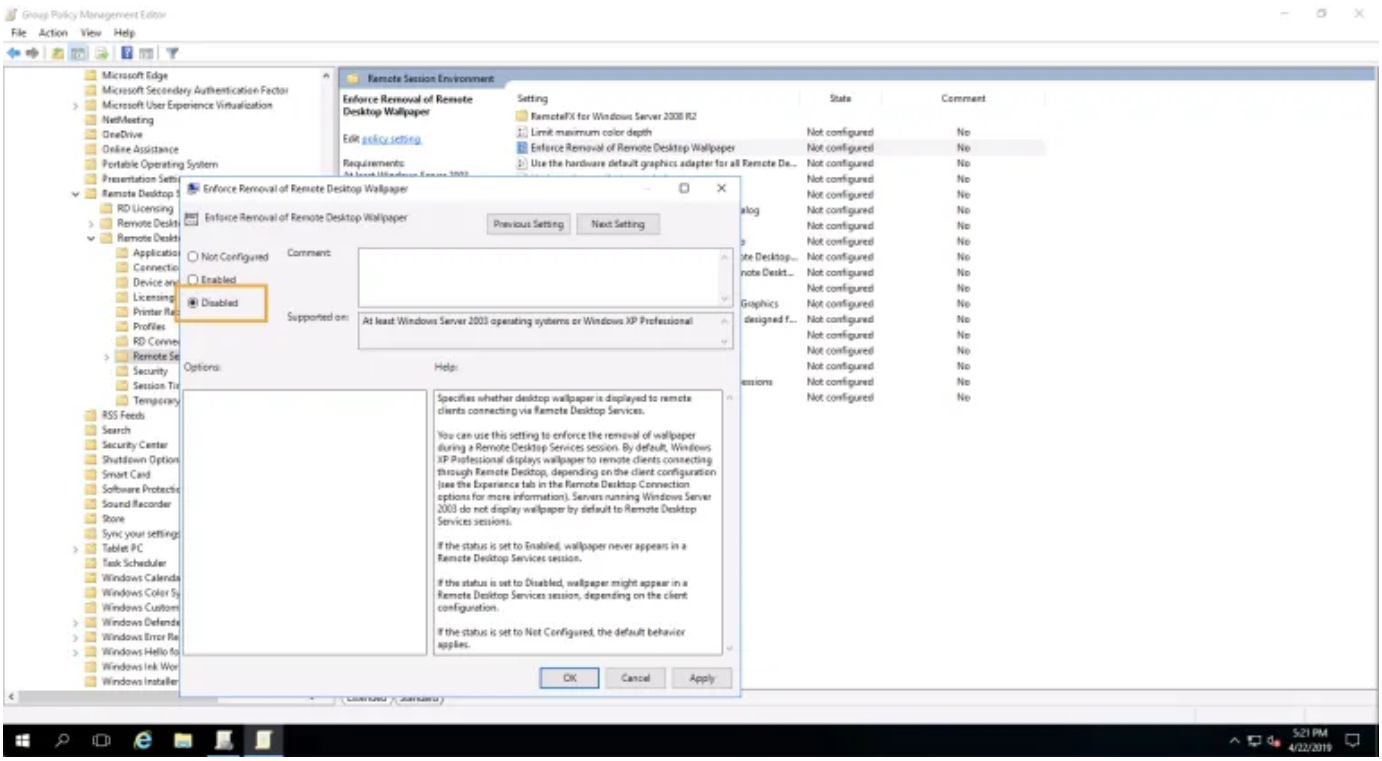
By default remote sessions have Wallpaper display disabled to improve performance. The result is a black wallpaper that users often wish to customize. This setting can be changed with a simple GPO edit

Instructions:

1. Login to a platform server (e.g. CWMGR1) using level3 .tech account
2. Open Group Policy Management Console
3. Locate the rdsh GPO (labeled as "company code" rdsh (e.g. "xyz1 rdsh")) Right click "xyz1 rdsh" GPO, choose edit
    a. In Azure AD Domain Services the GPO is called "AADDC "Computers > Cloud Workspace Computers"
4. Modify the Policy: Computer Configuration > Policies > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Remote Session Environment > Remove remote desktop wallpaper set this to Disabled


Azure AD
Internal AD





Troubleshooting Printing Issues

Error

Printing to the local printer from the cloud desktop is not working.

Remote Desktop Services with ThinPrint

VDS optionally includes ThinPrint for Remote Desktop Services (RDS) deployments. The software and licensing are automatically configured at initial deployment. If ThinPrint is in use, the following sections can help troubleshooting issues with printing.

Cause

There are a variety of methods to connect to the cloud desktop. These method differ in how they perform printing functions and thus knowing which type of access is in use is necessary for troubleshooting:

1. Using CloudJumper's access client on a Windows device
    a. ThinPrint runs on the local device and relays communication between the printer and the cloud desktop
2. Using the HTML5 browser on any device
    a. The browser will present the printed document as a PDF to download and print locally
3. Using a manually configured RDP client (usually) on a Mac or Linux machine
    a. Local printers are shared with the cloud desktop by manually configuring "Local Resources" in the RDP Client.

Resolution

1. Attempt to print a document from the local device to confirm that the local device is successfully connecting

to the printer.

2. Uninstall and re-install ThinPrint if using the Access Client on a Windows device. https://www.thinprint.com/en/resources-support/software/clientsandtools/
3. Make a note of the access type and the results of the first two steps in a new case with CloudJumper Support.

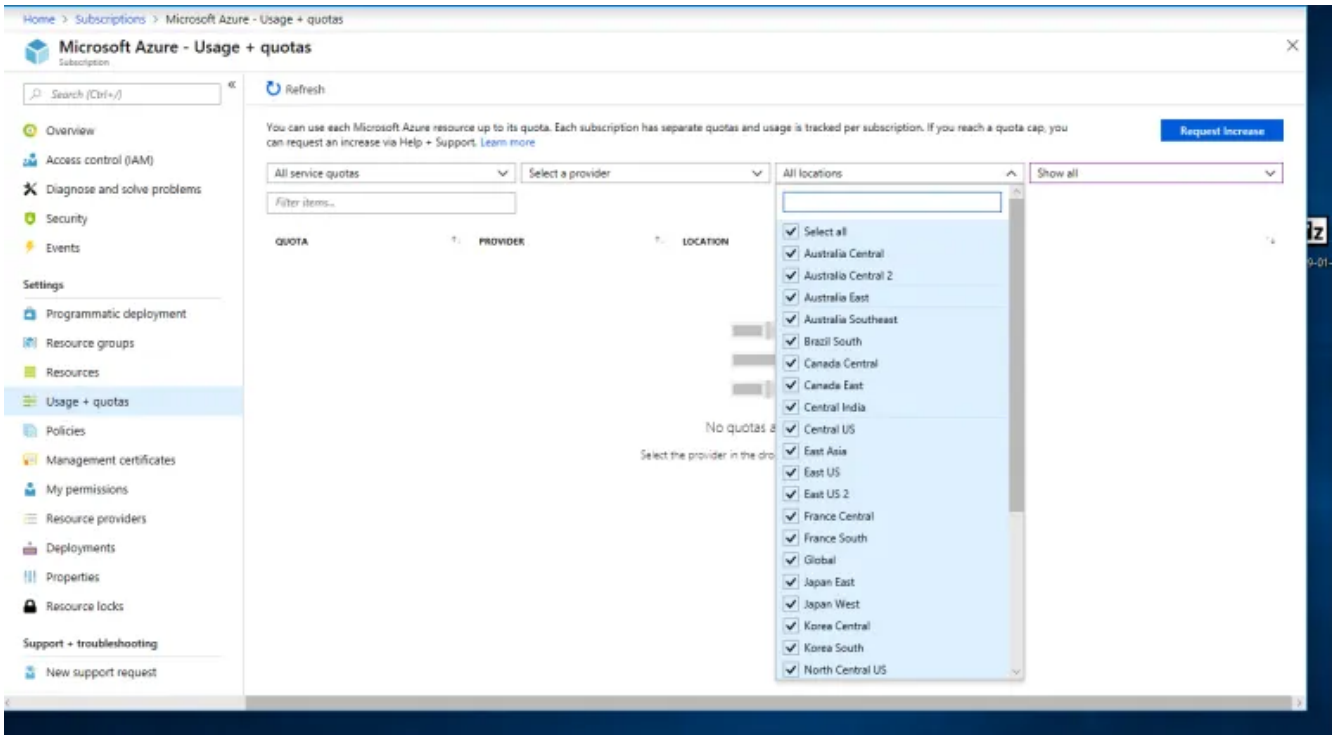
Azure Virtual Desktop

VDS does not implement any printing solution or unique printing configuration for AVD environments. Printing questions should be directed to Microsoft or (if one was implemented) the printing technology vendor.

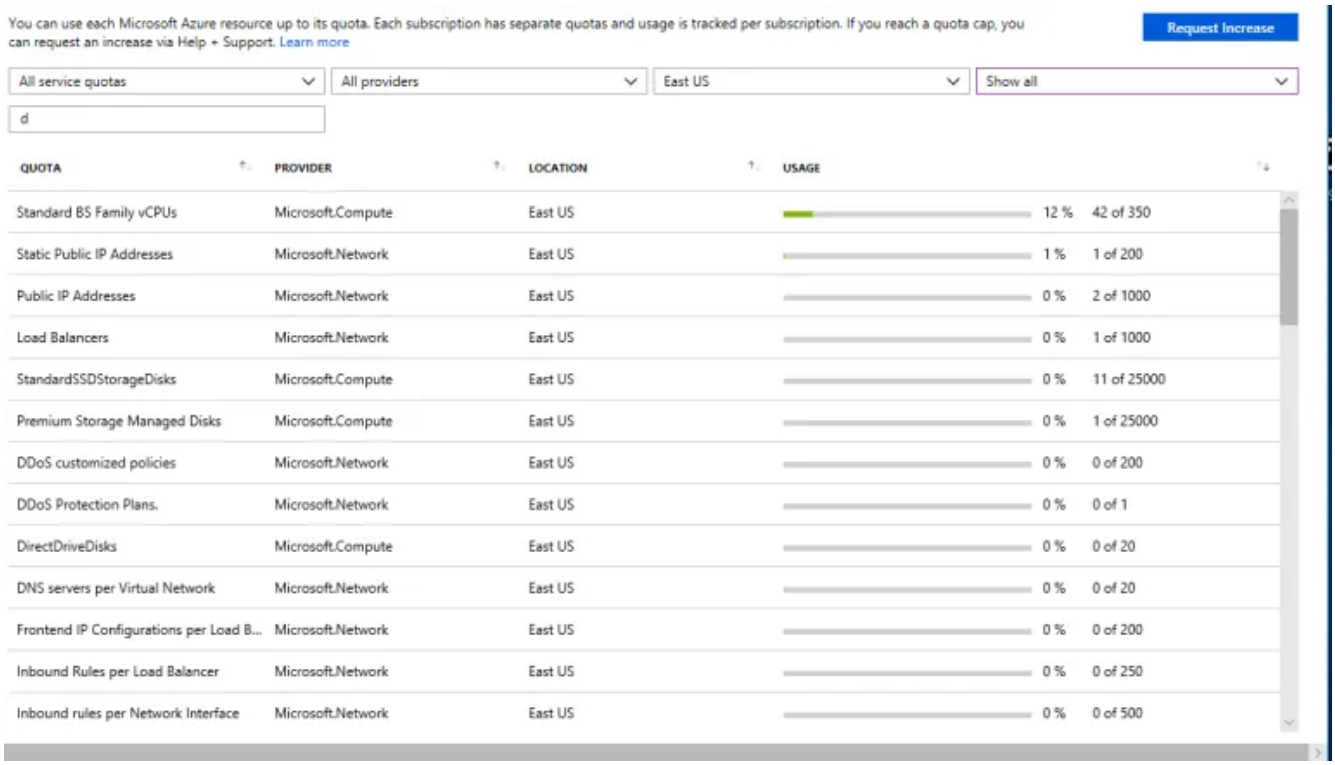
Azure vCPU Core Quota

View Current Quota

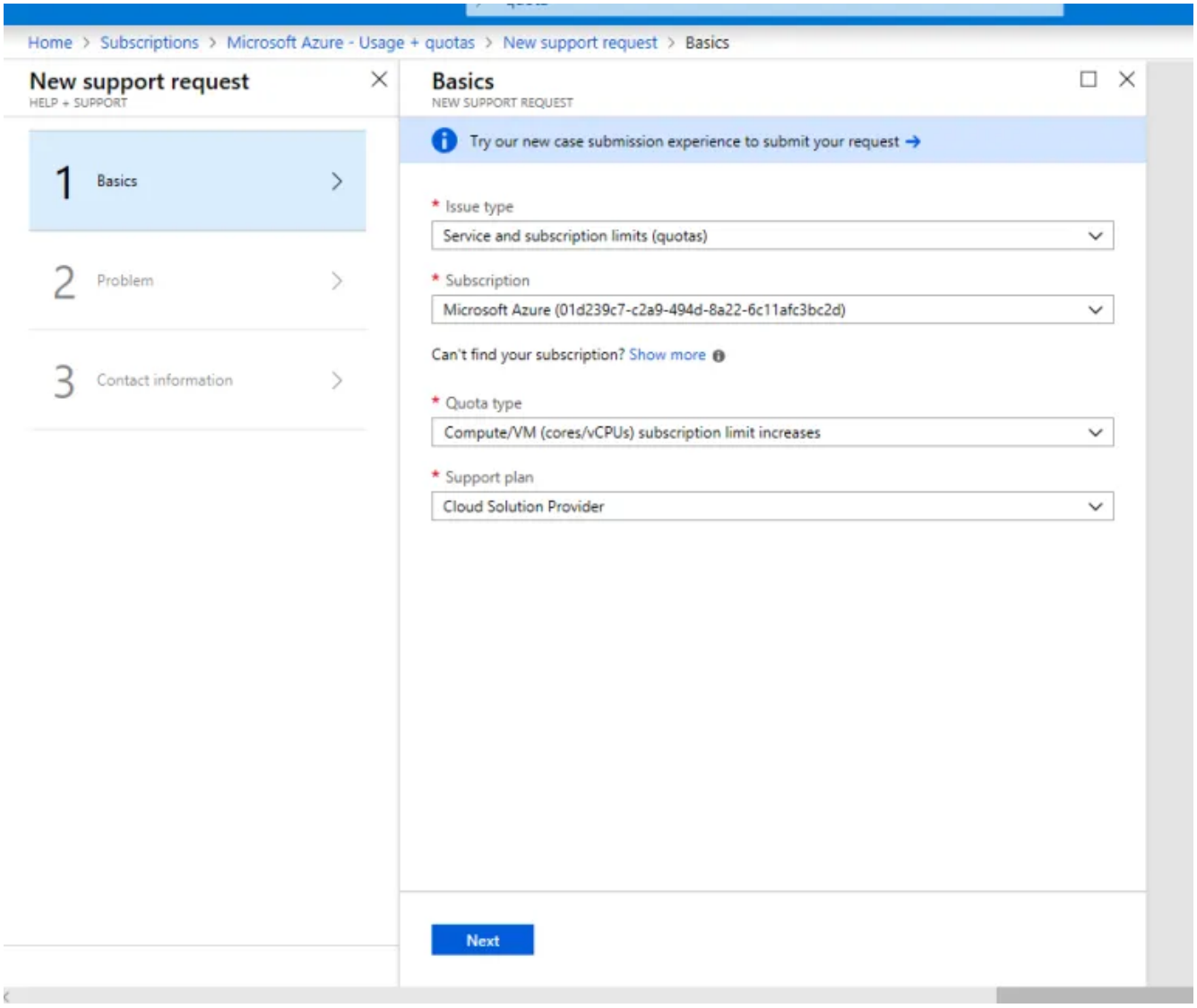
1. Log into the Azure console and navigate to the Subscriptions module and click Quotas. Next, select all providers in the providers drop-down, select show all in the far-right drop down and select the Azure region in which your Cloud Workspace is deployed.



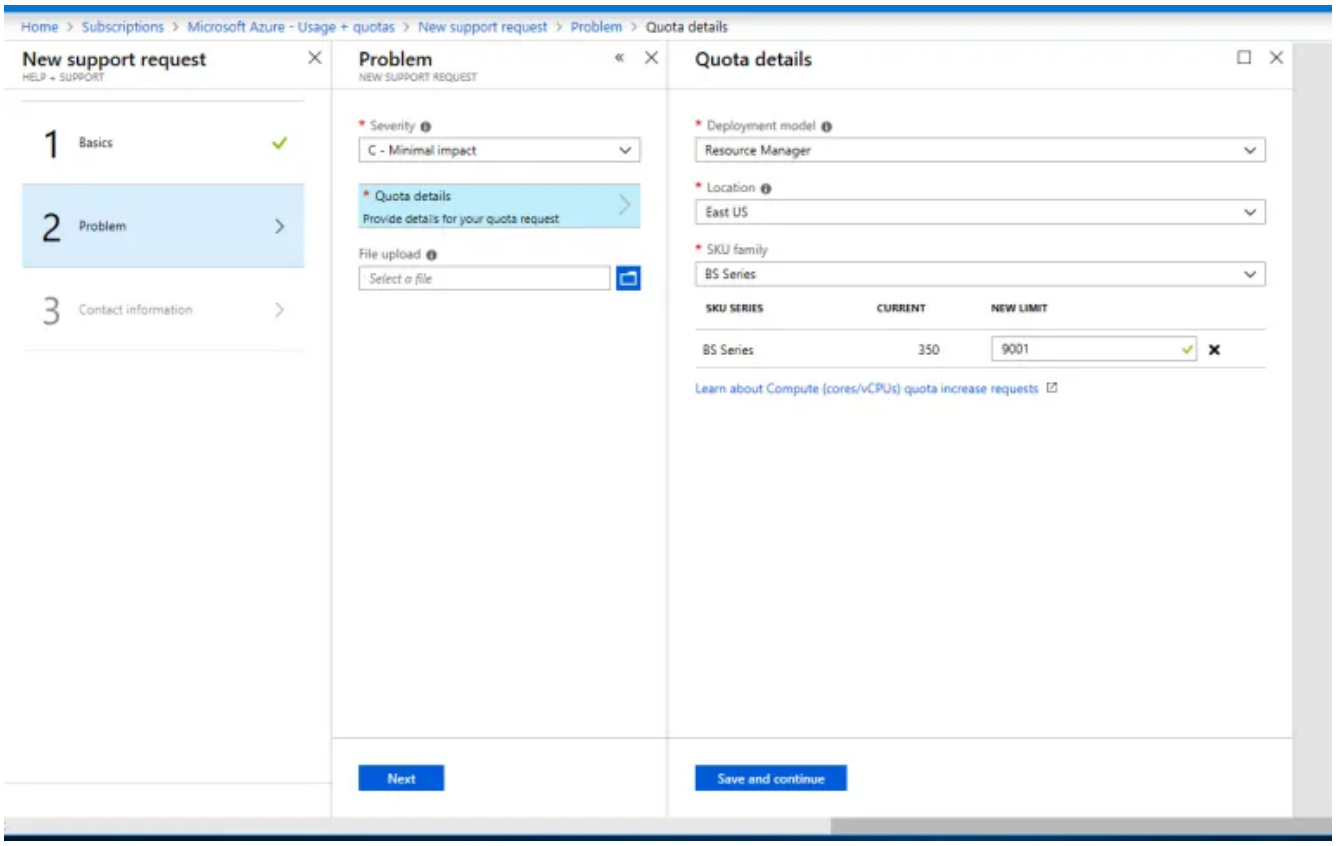
2. Then you'll see how much you're consuming vs. how much quota you have available. In the image below, CloudJumper is consuming 42 CPUs out of the 350 CPUs available for the BS family of VMs.
Increasing Quota



3. If you want to increase your quota, click Request Increase and tell it what you want to increase (99% of the time this will be compute/CPUs).



4. Select the region your Cloud Workspace is deployed in and the VM family you want to increase quota for.



5. Enter your contact info and click Create to submit the request to Microsoft. They are usually VERY fast at increasing this.

Unlocking User Accounts

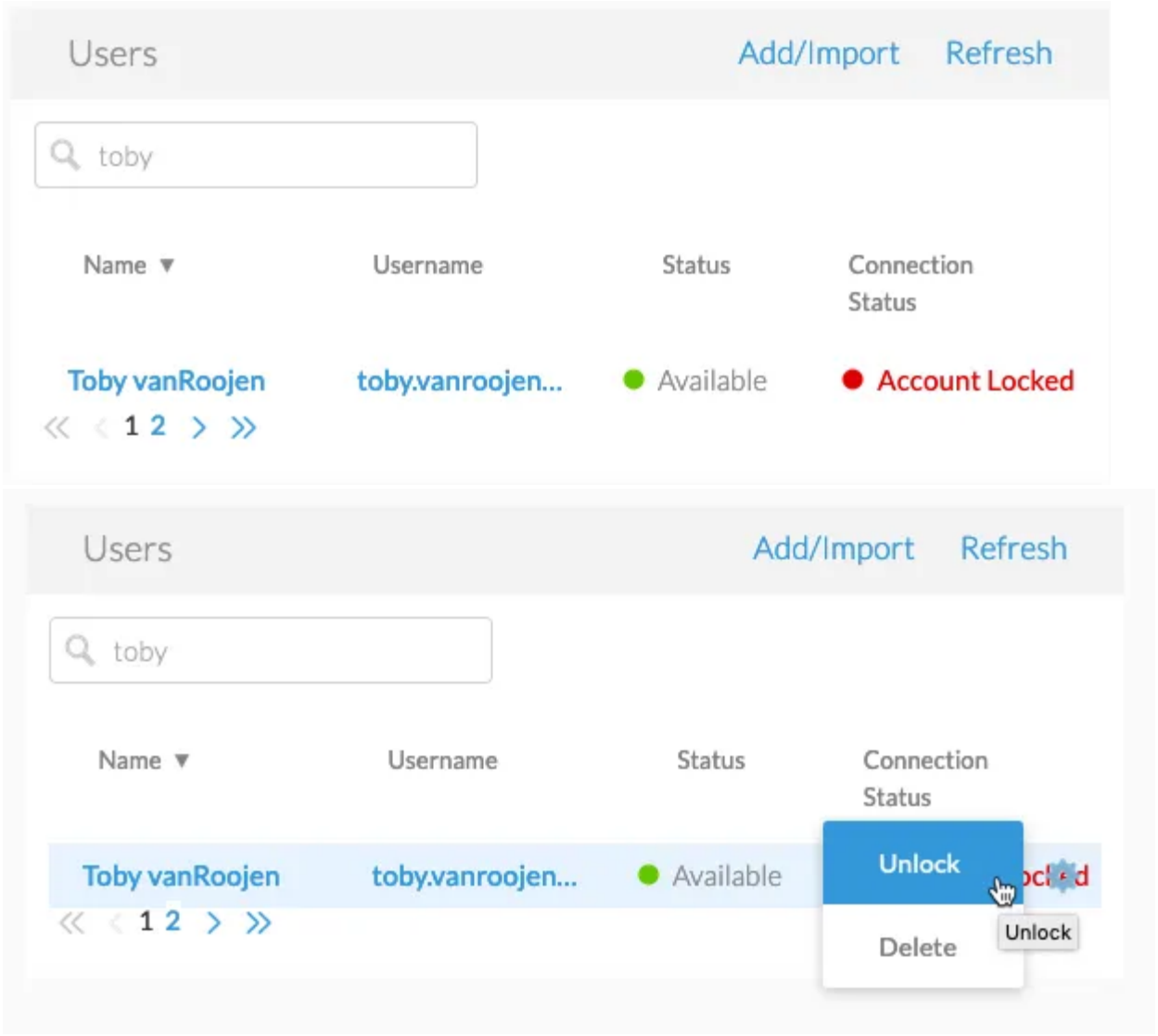
Overview

Unlocking a locked account for an End User is a simple process that resolves a moderately common issue that end users report.

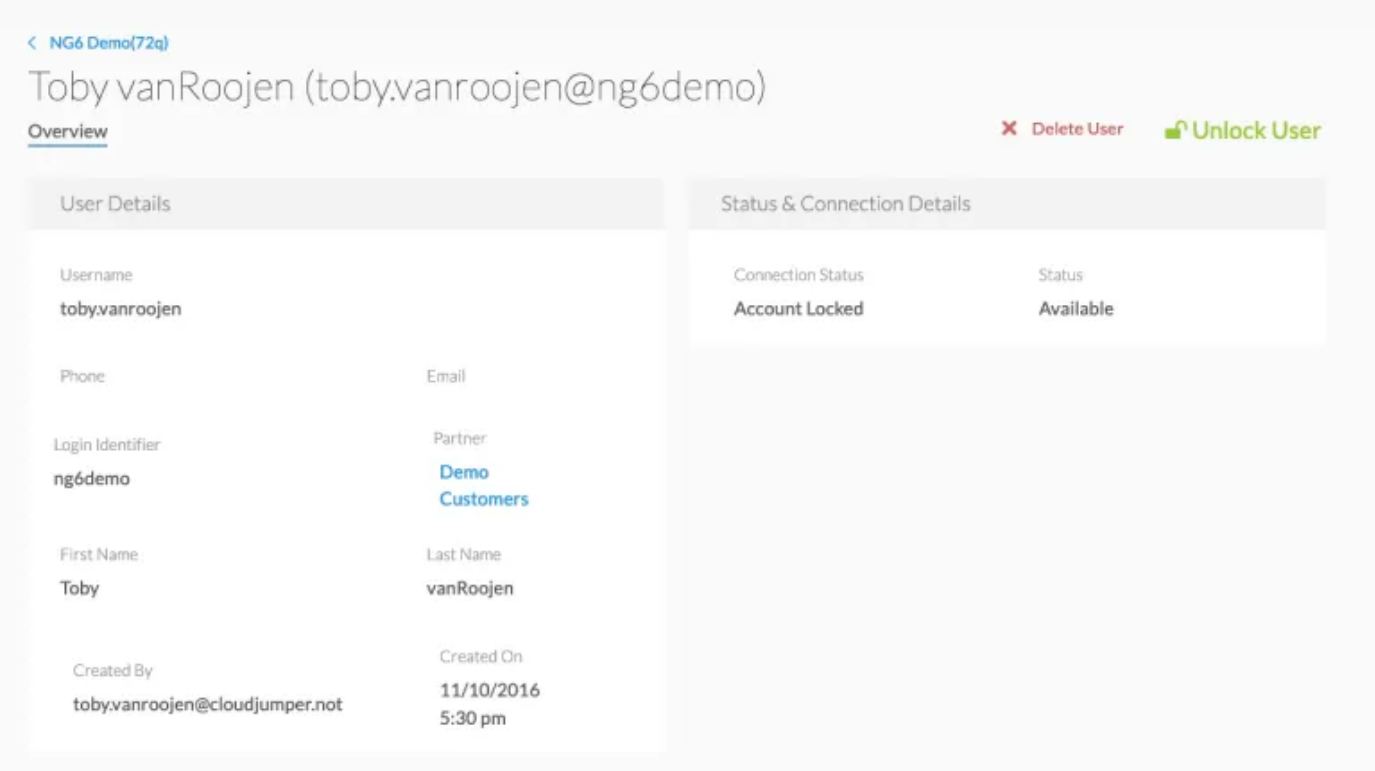
After four failed login attempts the User will be locked out. The duration is 30 minutes unless the customer account has password complexity enabled, in which case the lockout can only performed manually.

The user account can be unlocked from the list of users on the Users & Groups page in the Workspaces or from the User Detail page.

Users & Groups Page



User Detail Page



Troubleshooting Virtual Machine Performance

NetApp offers customers insight into troubleshooting server performance for users/apps. All companies consume resources differently based on the number of end users logged in at once, application use, if SQL Standard is installed vs. SQL Express, etc. so it is important to be able to review what is happening when a user reports performance issues.

Overview

Every app is different, and even the same software being run by the same number of users can have different resource consumption patterns. This is why it helps to understand the apps your users are running and what truly powers that app. Is it CPU, RAM or storage? These considerations will help focus your troubleshooting.

In our experience, these have proven to be generally true statements to help you begin:

```
CPU: this is usually the culprit/limiting factor if the app in question is
home-grown and/or an Excel issue
RAM: this is usually the culprit/limiting factor if SQL Standard is used
Storage: this is usually a contributing factor if disk consumption is
greater than 90%.
```

If SQL Express is used, it is likely a limiting factor – it limits RAM consumption to 1 GB, which will may be under the software vendor's required specs.

Using nightly resource reports

VDS sends nightly reports with information about each VM. There is a lot of useful information in that report, including recommendations on whether to increase or decrease resources. Here are a few excerpts:

This image shows whether you should increase or decrease CPU/RAM on VMs for a given workspace.

Company Code	Pool	Run Date PDT	Allocation Type	# Servers	# Users	Max Active Users	Ram GB Per User	CPU Per User	Max Ram %	Max CPU %	Recommended Change RAM	Recommended Change CPU	Ram GB	CPUs
[redacted]	[redacted]D1	2018-07-30 09:12 AM	Unknown	0	0	0	N/A	N/A	N/A	N/A	No Change	No Change	0	0
[redacted]	[redacted]D1	2018-07-30 09:12 AM	Unknown	0	0	0	N/A	N/A	N/A	N/A	No Change	No Change	0	0
[redacted]	SHARED	2018-07-30 09:12 AM	Fixed	0	0	0	N/A	N/A	N/A	N/A	Need More Data	Need More Data	6	2

In the image below, we can see that there is a column that shows how long it has been since the server has been rebooted.

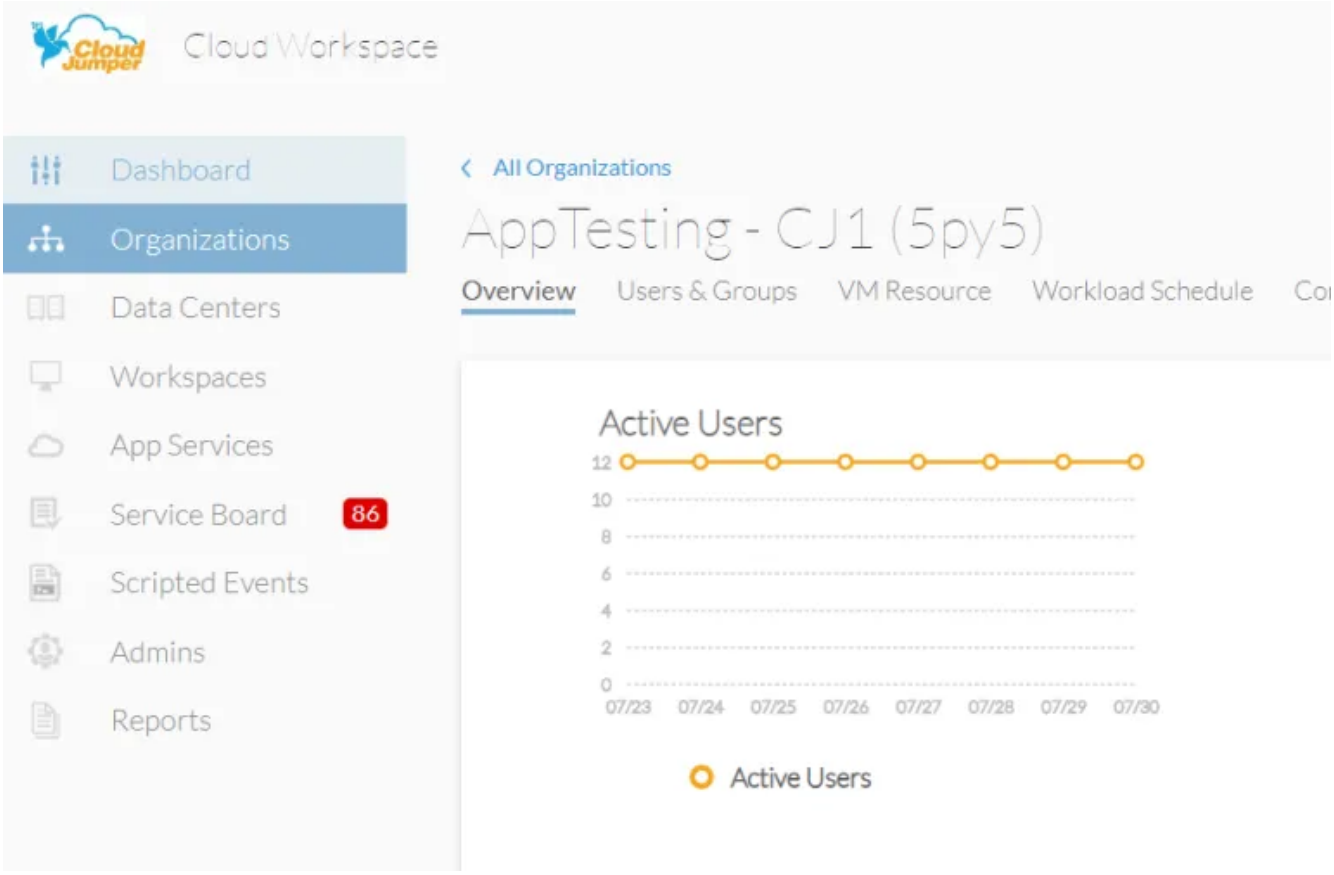
Time Since Last Reboot (dd:hh:mm)	Time Zone	RAM GB	CPUs
38:20:17	(UTC-08:00) Pacific Time (US & Canada)	4	2
146:00:46	(UTC-08:00) Pacific Time (US & Canada)	4	2

In this image we can see storage provisioned vs. consumed – this becomes a good topic to investigate briefly at first or once you have validated that CPU/RAM are not the issue.

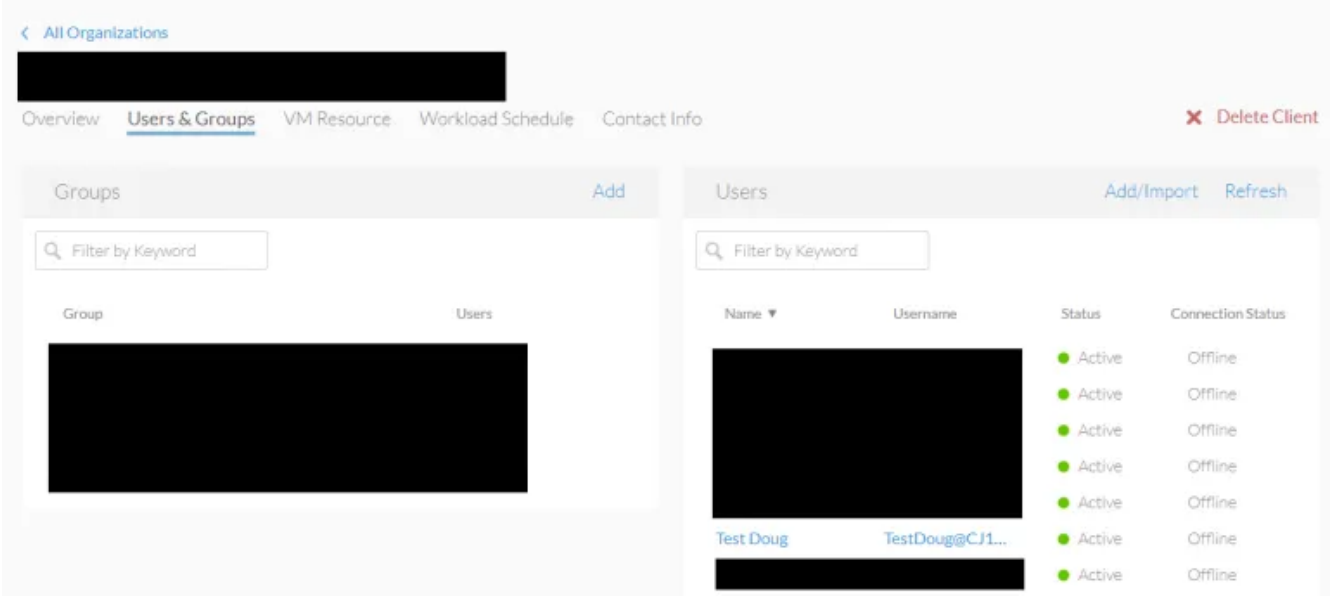
Drive Total Space GB	Drive Used Space GB	Drive Free Space GB
63	15.63	47.82

Viewing CPU/RAM resource consumption in real-time

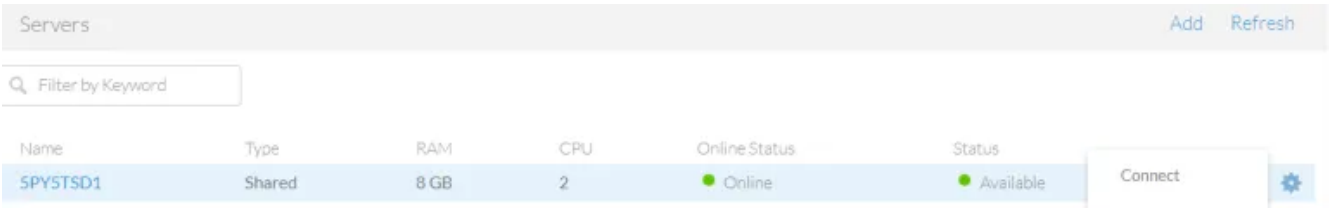
1. Log into VDS, then click the Organizations module and select the organization in question.



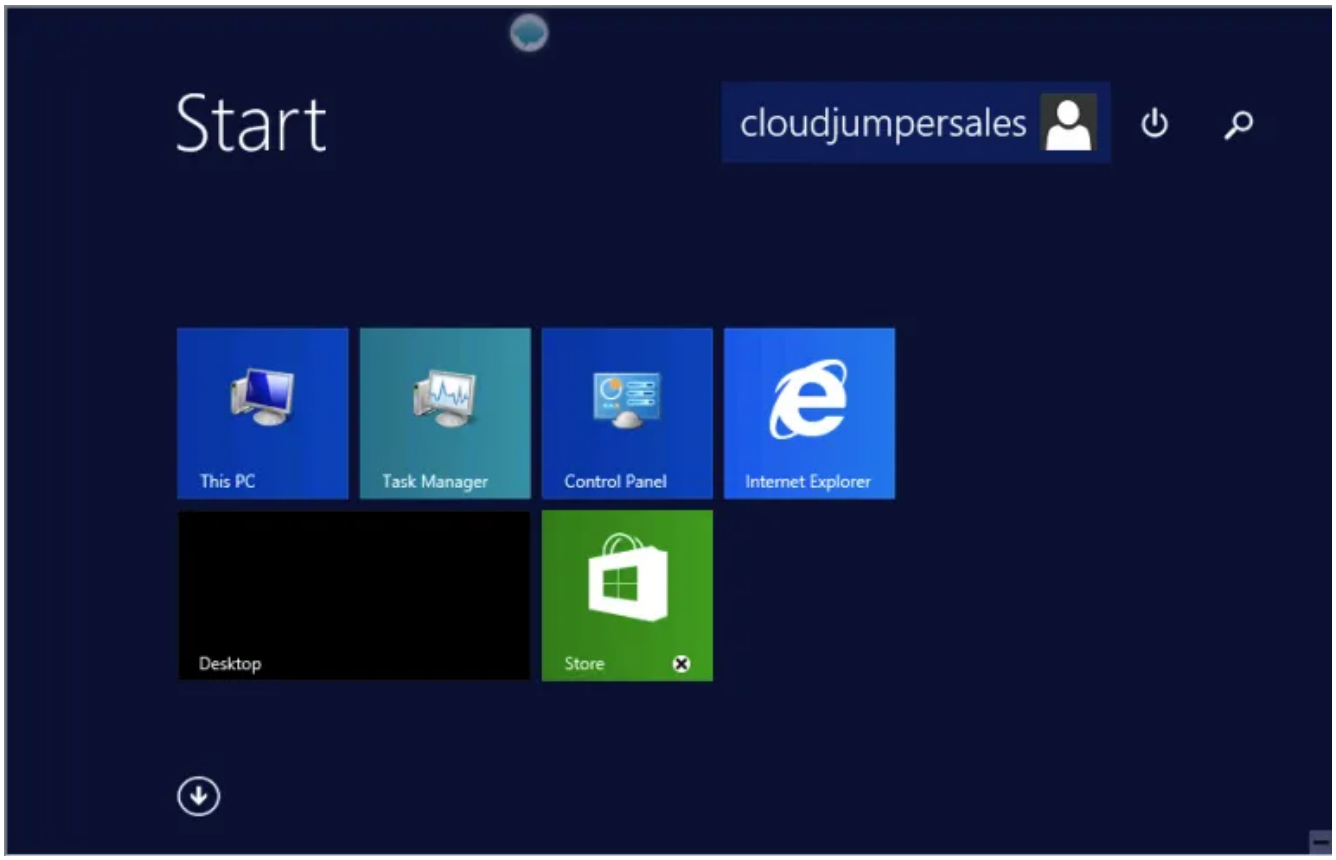
2. You can locate what server the user is logged into by locating them in the users section.



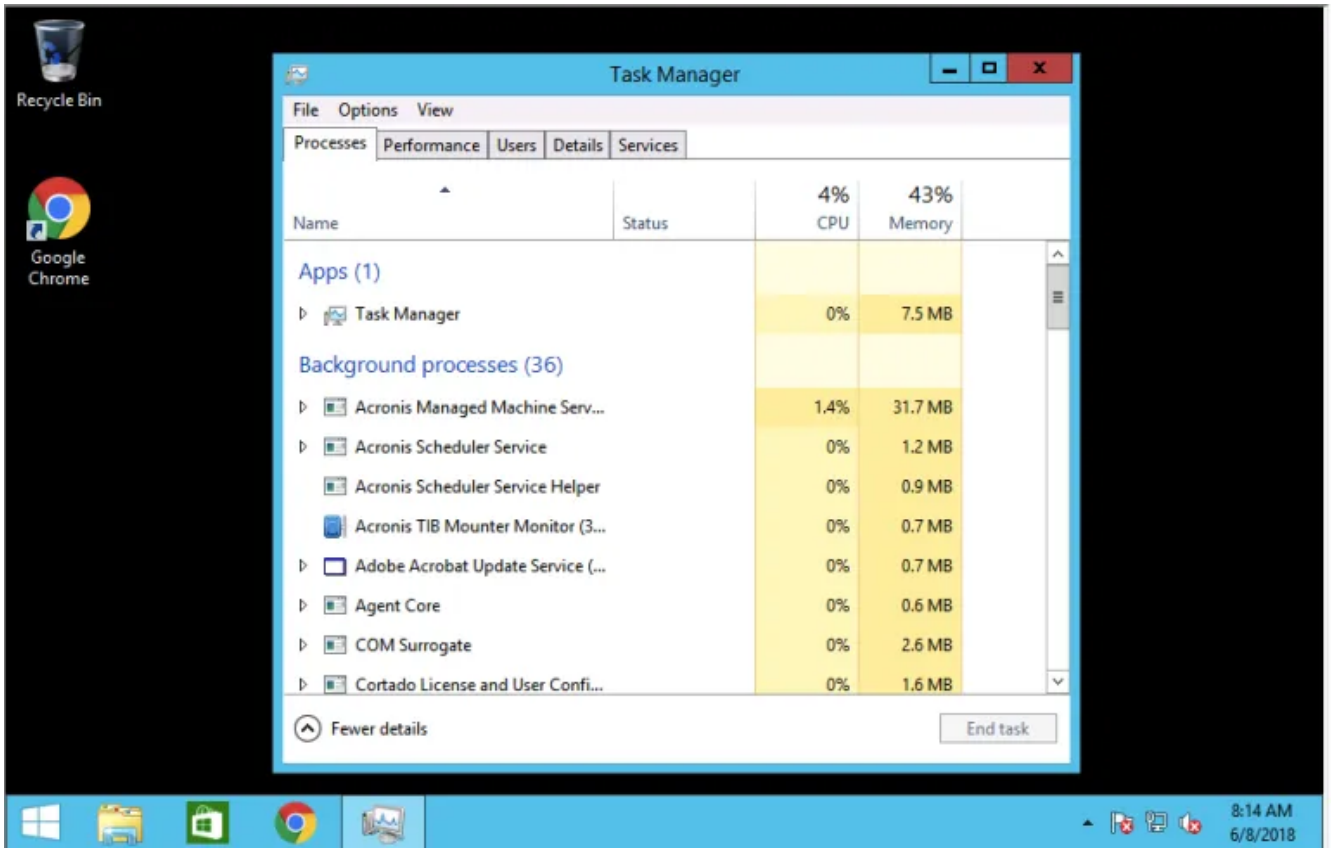
3. Next, scroll down until you see the Servers section – locate the server the user reporting the issue is logged into and click the settings wheel, then connect.



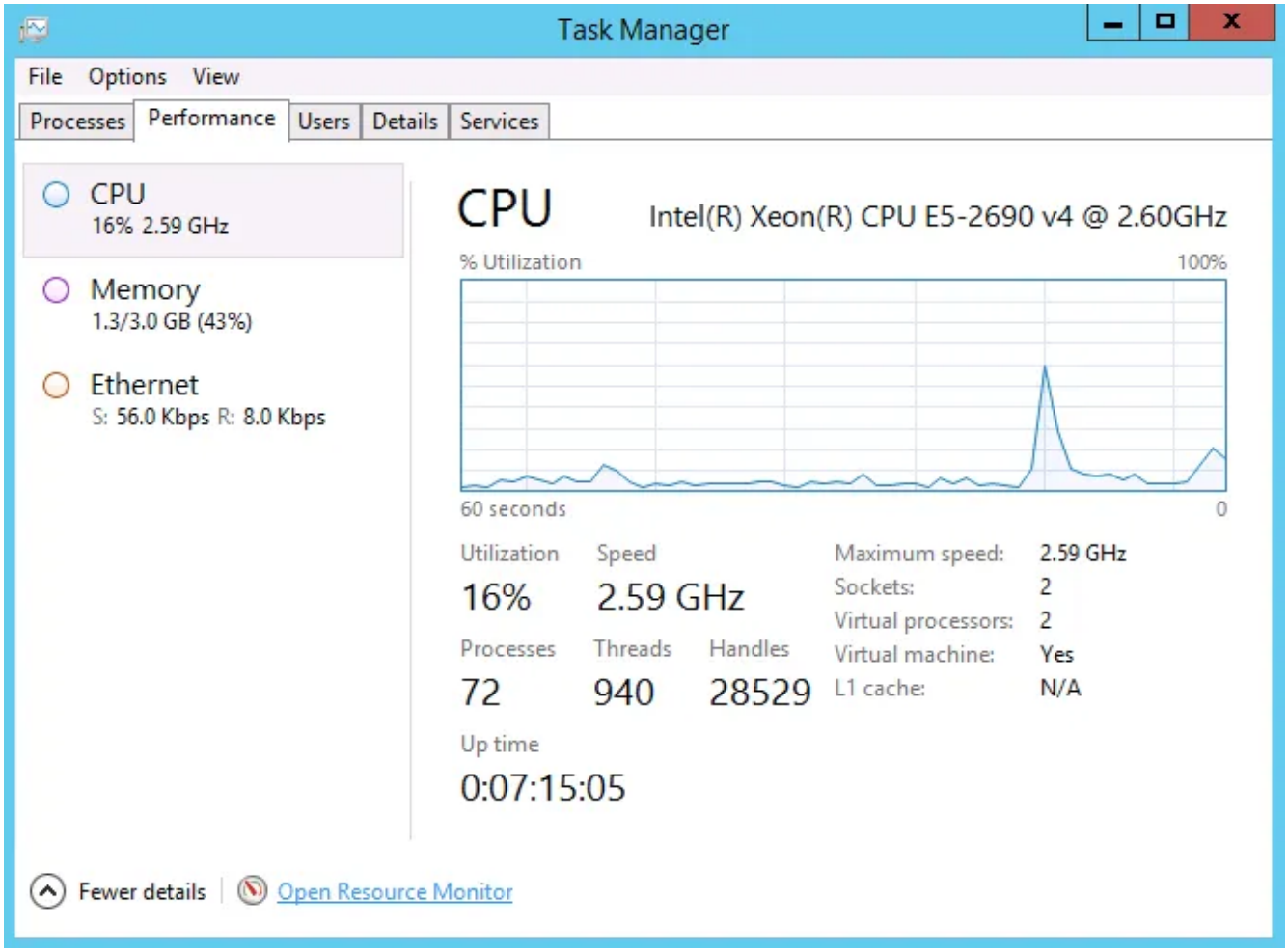
4. Once you've connected to the server, click the Start button. Next, click Task Manager.



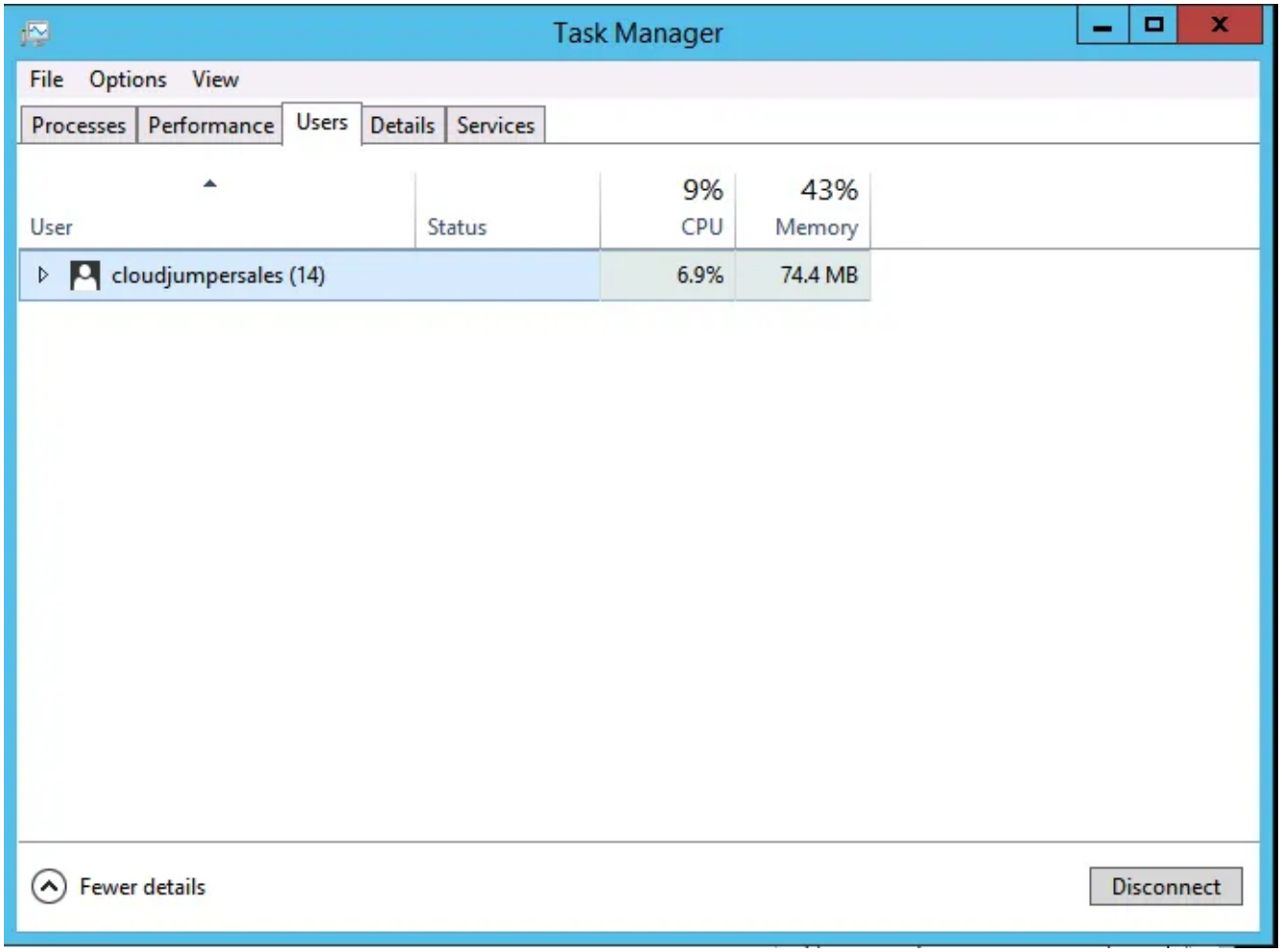
5. The Task Manager gives a wealth of insight into what's happening, right at that moment. This is the absolute best way to see what's affecting your users at the moment they report an issue to you.
6. You can review the processes running on the server, identify which if any are causing the issue and either communicate with the Customer or end the processes on the spot.



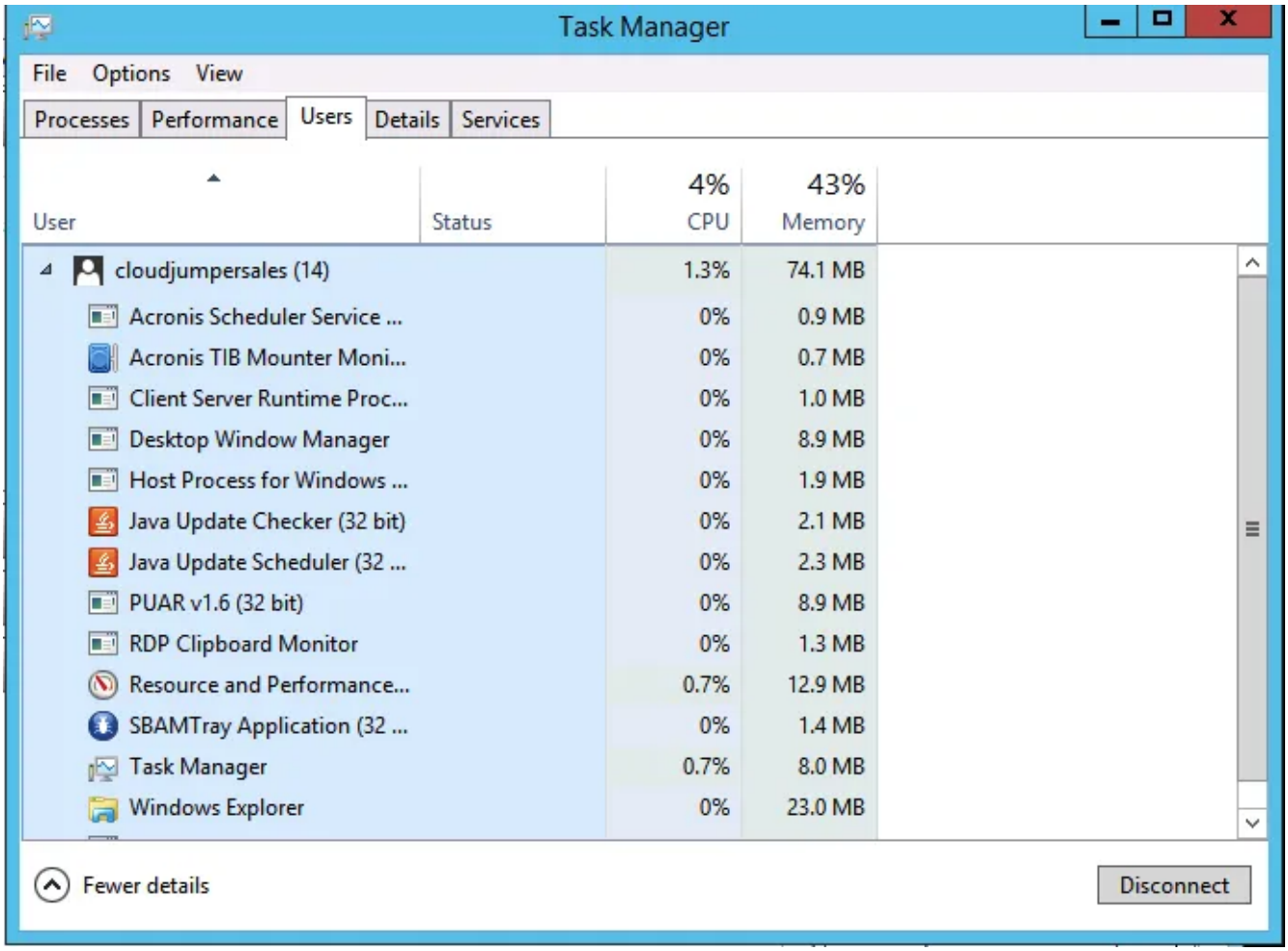
7. You can also view the Performance tab to show what's happening, live. This is a tremendous troubleshooting step – asking End users to repeat the steps they took to cause a performance issue, then seeing what happens. Similarly, if they follow general advice (close excess Chrome browser tabs, as Google Chrome tabs are a common resource consumer) you can see resource consumption decrease.



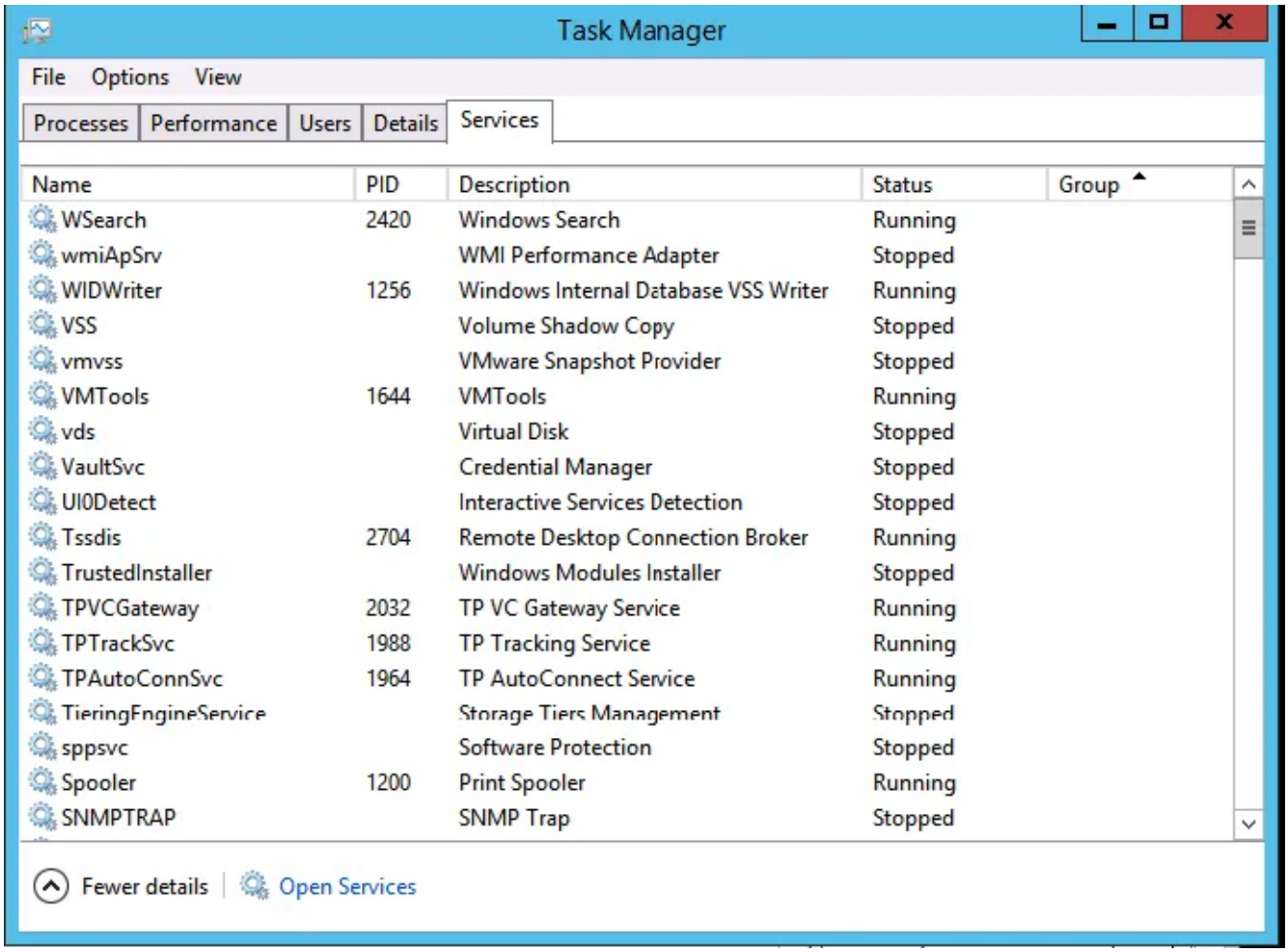
8. The users tab can show you which user, if any, is consuming the resources causing a spike in consumption.



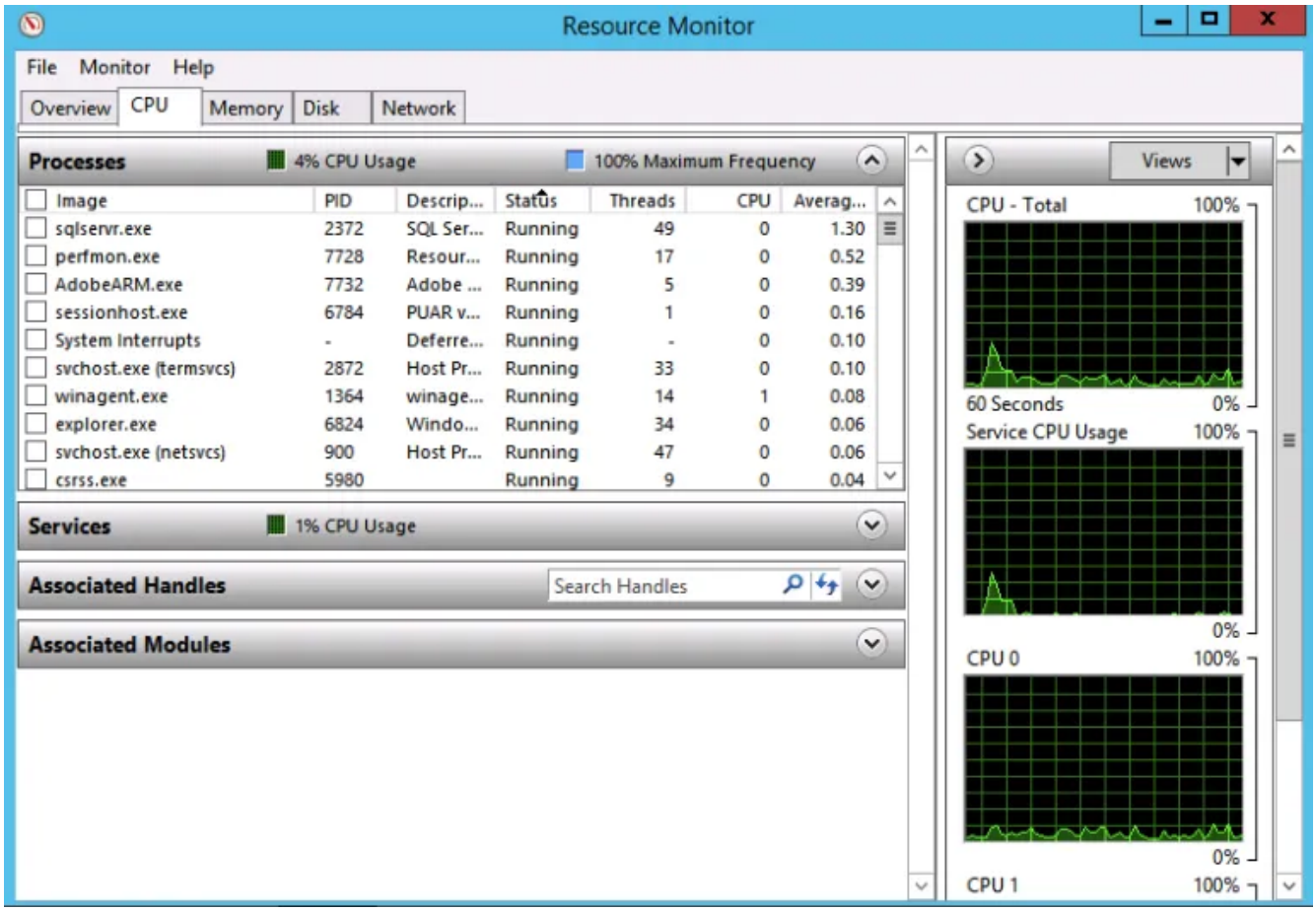
9. You can expand each End user to see which specific processes they’re running and how much each one is consuming.



10. Another option is viewing which services are running.



11. Customers can also open the Resource Monitor to investigate in more detail.



Considering storage performacne

One of the more common causes of vm performance issues is insufficient disk performance. Standard (and even SSD) disks are not designed to handle the high I/O load demanded by VDS workloads. User logins tend to happen in bunches and each one demands significant I/O as profiles and settings are loaded. NetApp's high performing storage technologies such at Azure NetApp Files, CVO and CVS are particularly well suited for this workload and should be considered the default option for VDS workloads.

Considering storage consumption

Microsoft has a long-held best practice against allowing disk consumption on any drive to exceed 90%. In their eyes, this causes performance to plummet and can cause a number of other challenges, such as not having enough storage for backups to complete and not allowing users to save their work.

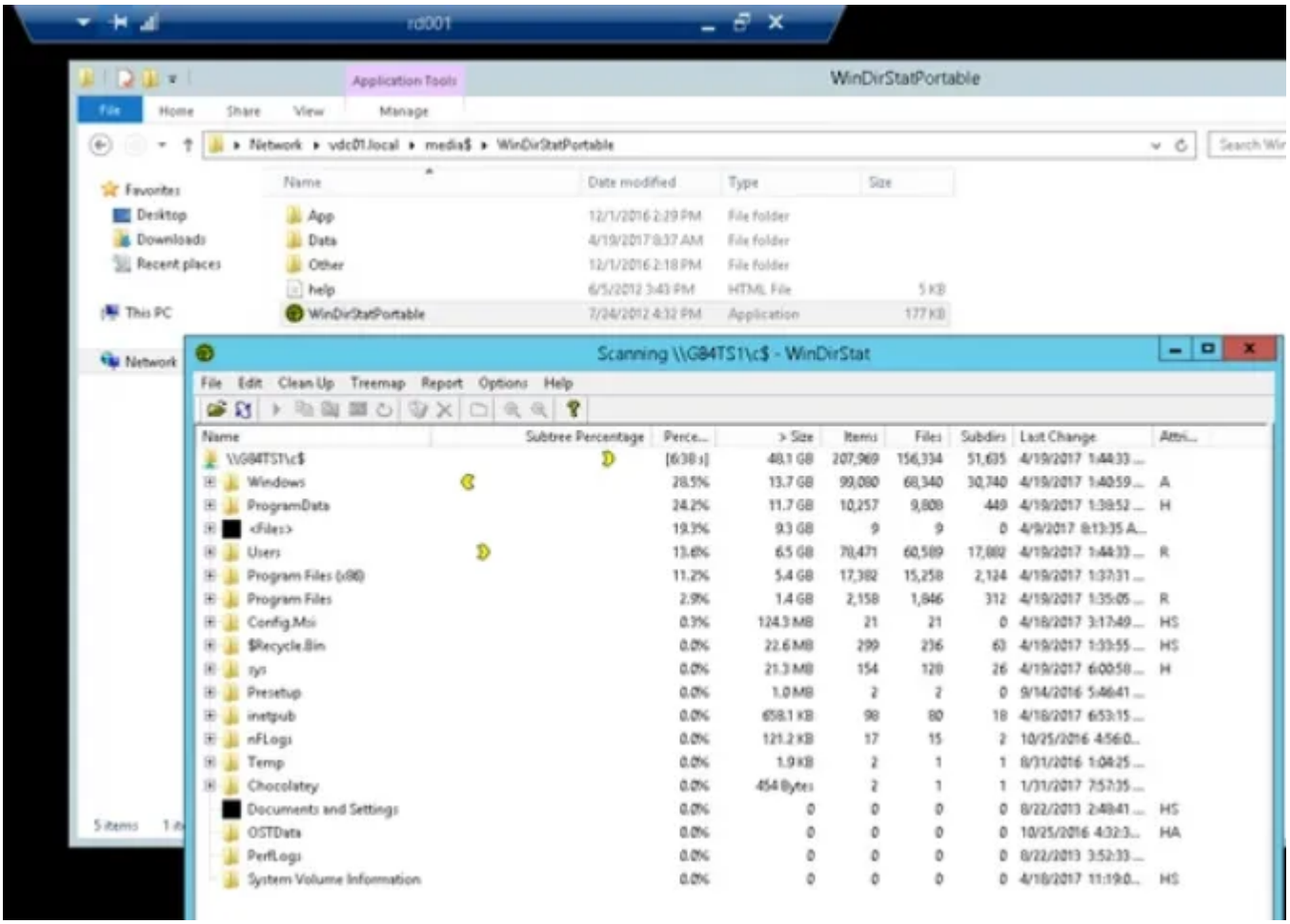
RMM tools can offer storage monitoring services, including the ability to set thresholds and alerts. If storage becomes a challenge for you, working with your RMM vendor to enable theses types of alerts is recommended.

For deeper investigation, install software to review drive consumption.

From conversations with customers, Windirstat or Treesize have proven to be the preferred applications for inspection of drive consumption.

Windirstat can inspect a full drive over the network if there is insufficient space to install/run an app locally or login is blocked:

+



DNS Forwards for Azure ADDS & SSO via O365 identity

Overview

Users can’t access company websites on primary email domain.

For Example, NetApp employees in VDS workspaces can’t access netapp.com if their SSO account is user@netapp.com

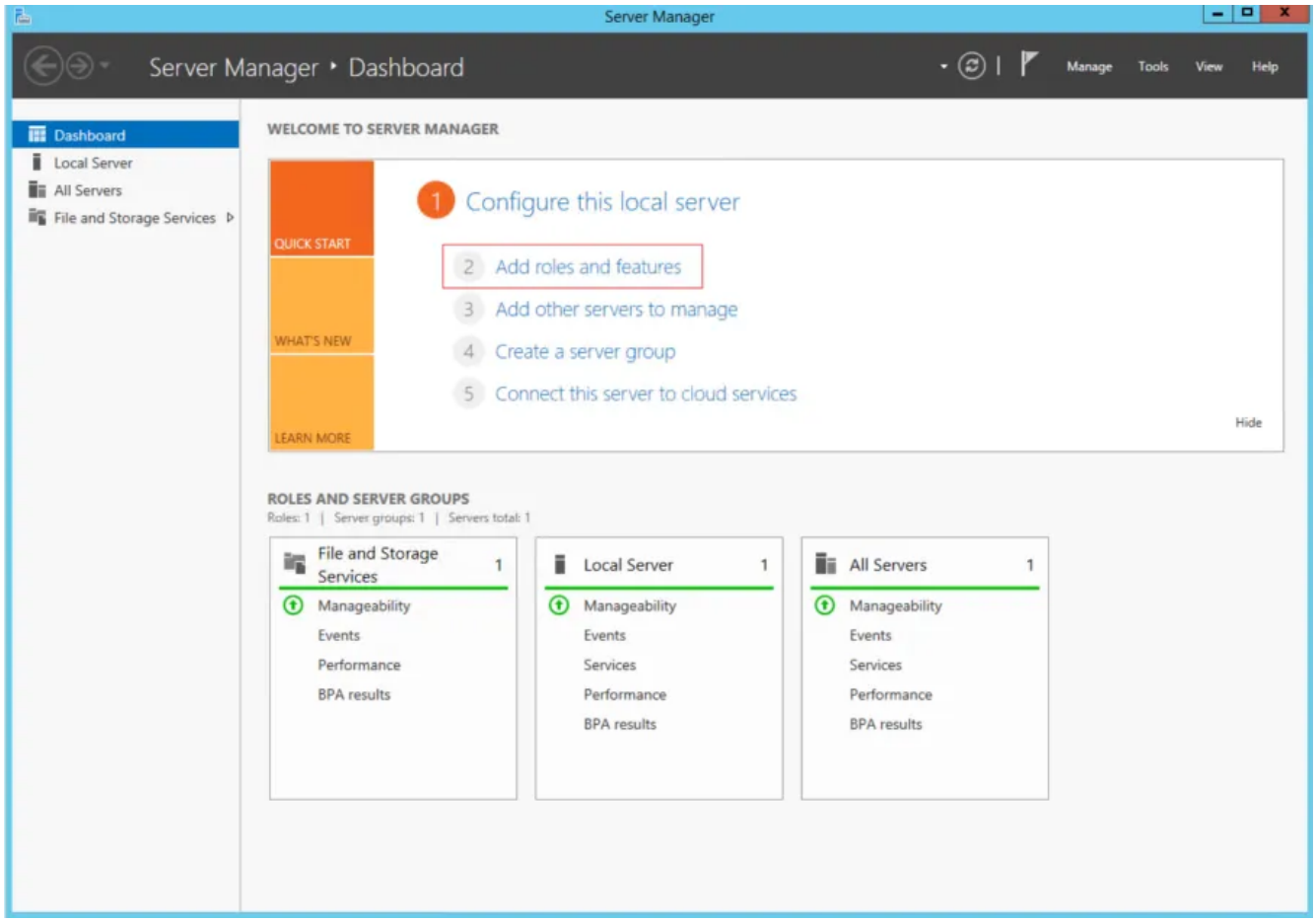
Dedicated VDS deployments use the internal domain of the Azure tenant.

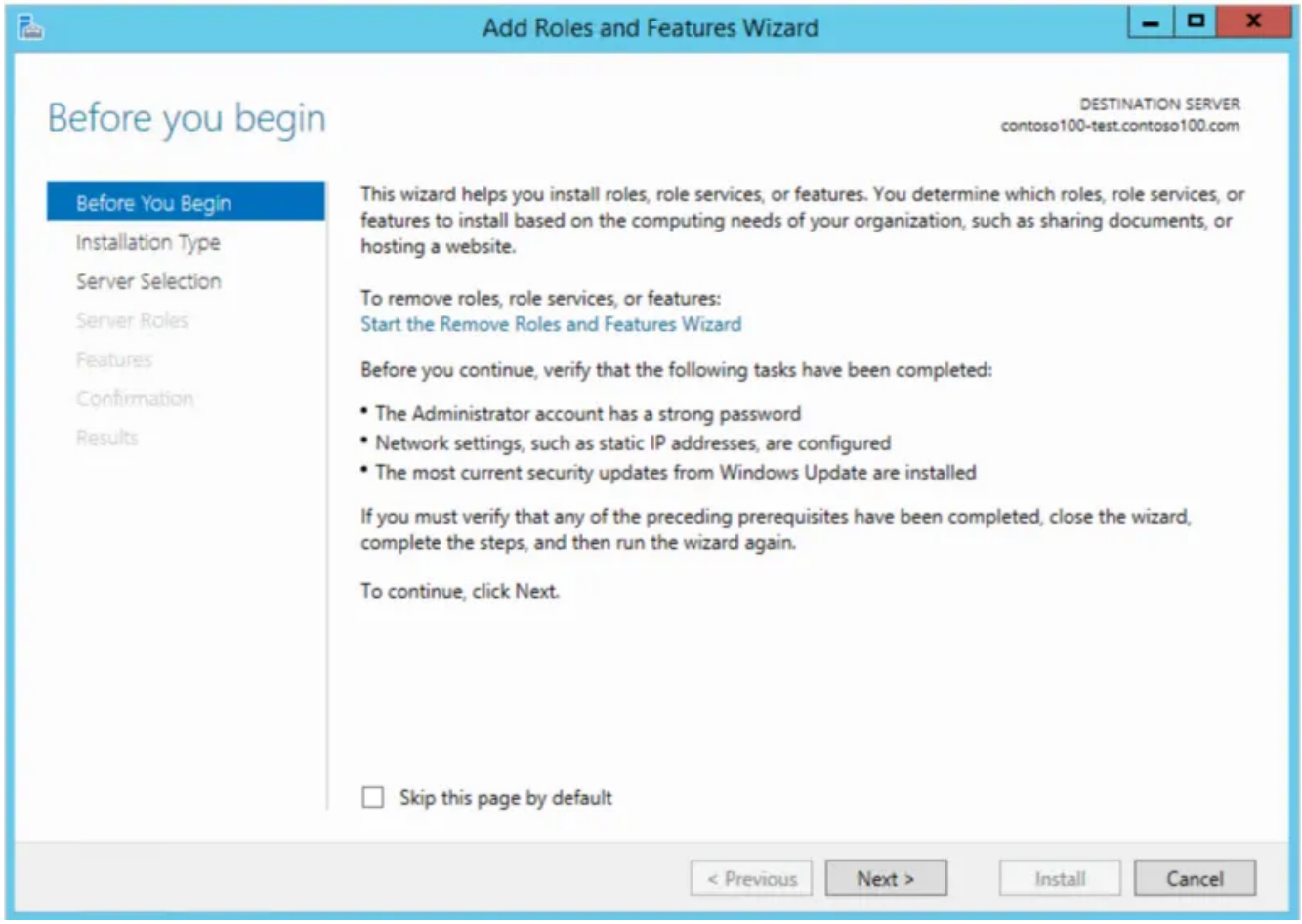
Resolution

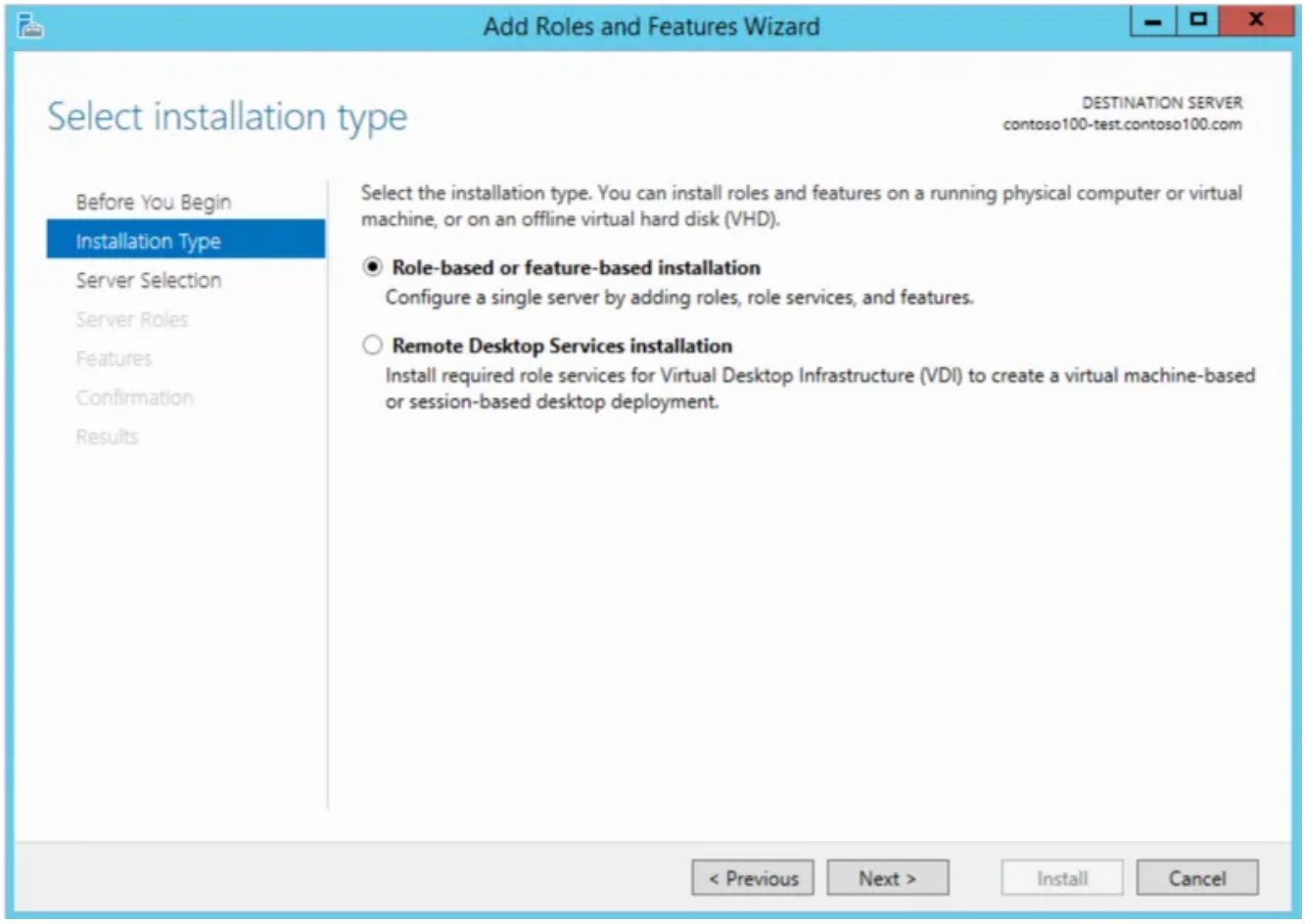
To resolve this, the Organization’s team that manages DNS will need to create a DNS forward lookup zone for your internal domain to allow it to resolve the the correct external IP (for NetApp’s purpose, this would let NetApp employees browse to netapp.com from within their virtual desktop).

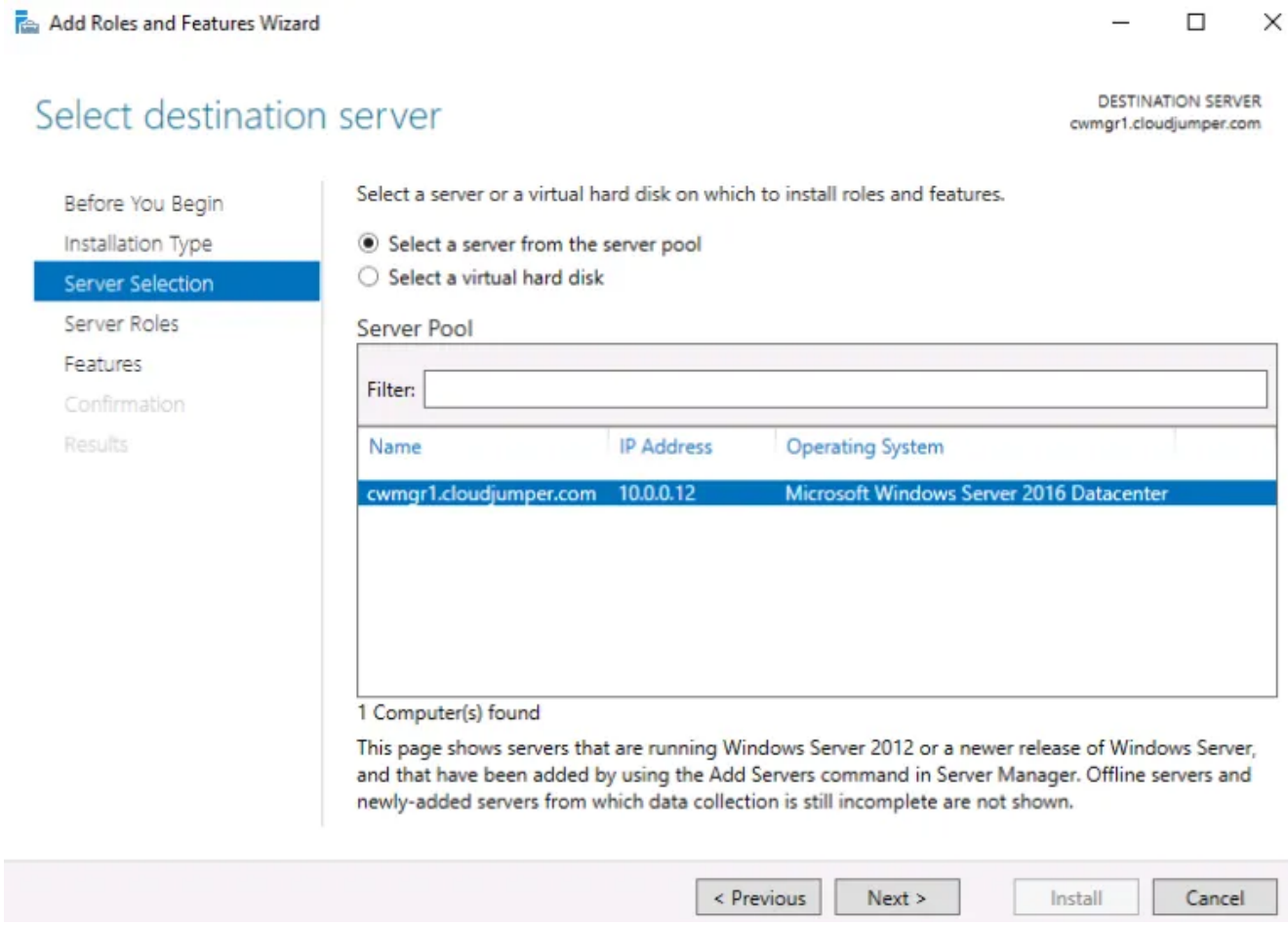
Step by Step Guide

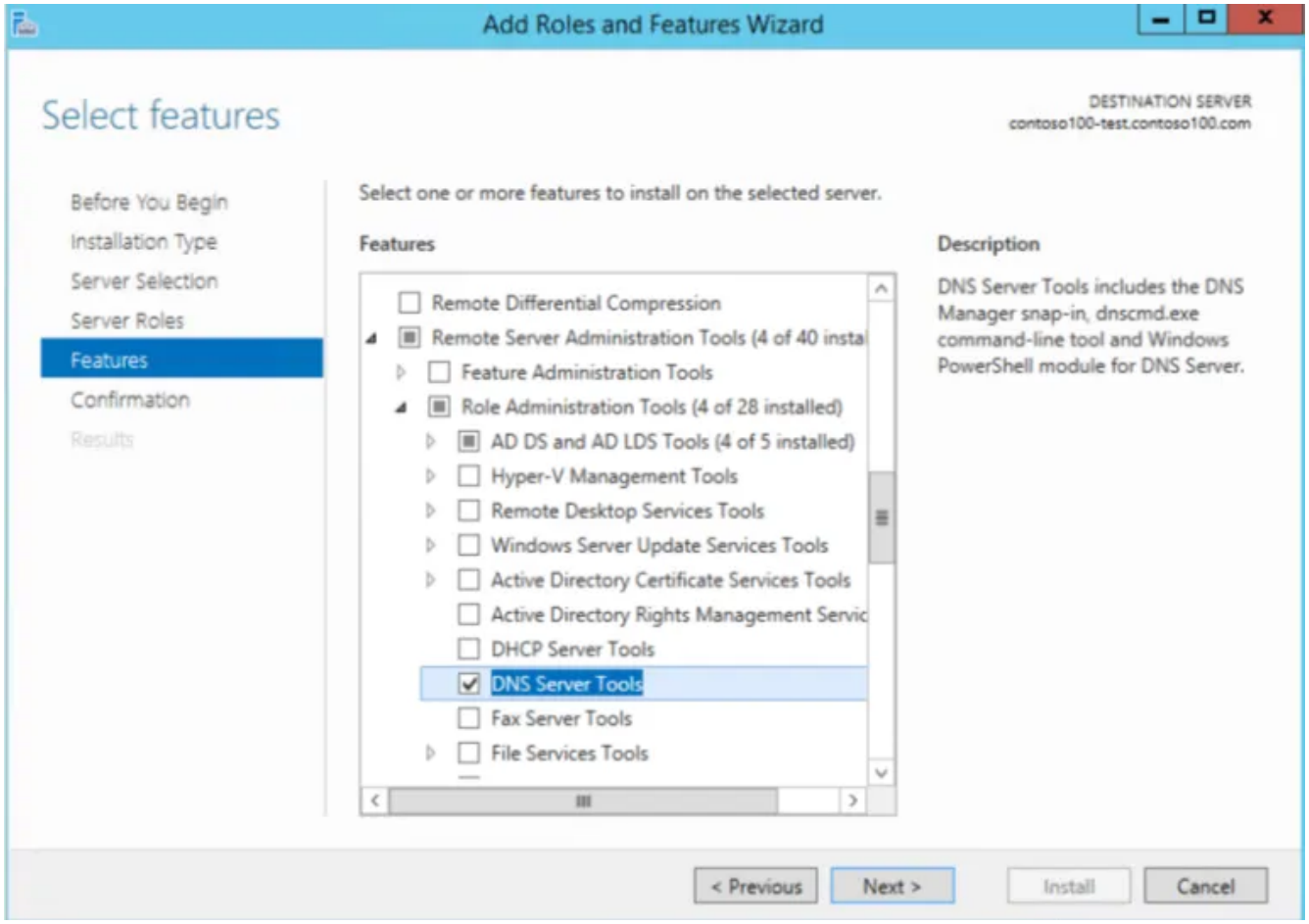
1. Install the DNS Server Tools on CWMGR1 – this will allow you to manage DNS.


Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide
ROLES AND SERVER GROUPS
Roles: 1 | Server groups: 1 | Servers total: 1
File and Storage Services 1
Manageability
Events
Performance
BPA results
Local Server 1
Manageability
Events
Services
Performance
BPA results
All Servers 1
Manageability
Events
Services
Performance
BPA results

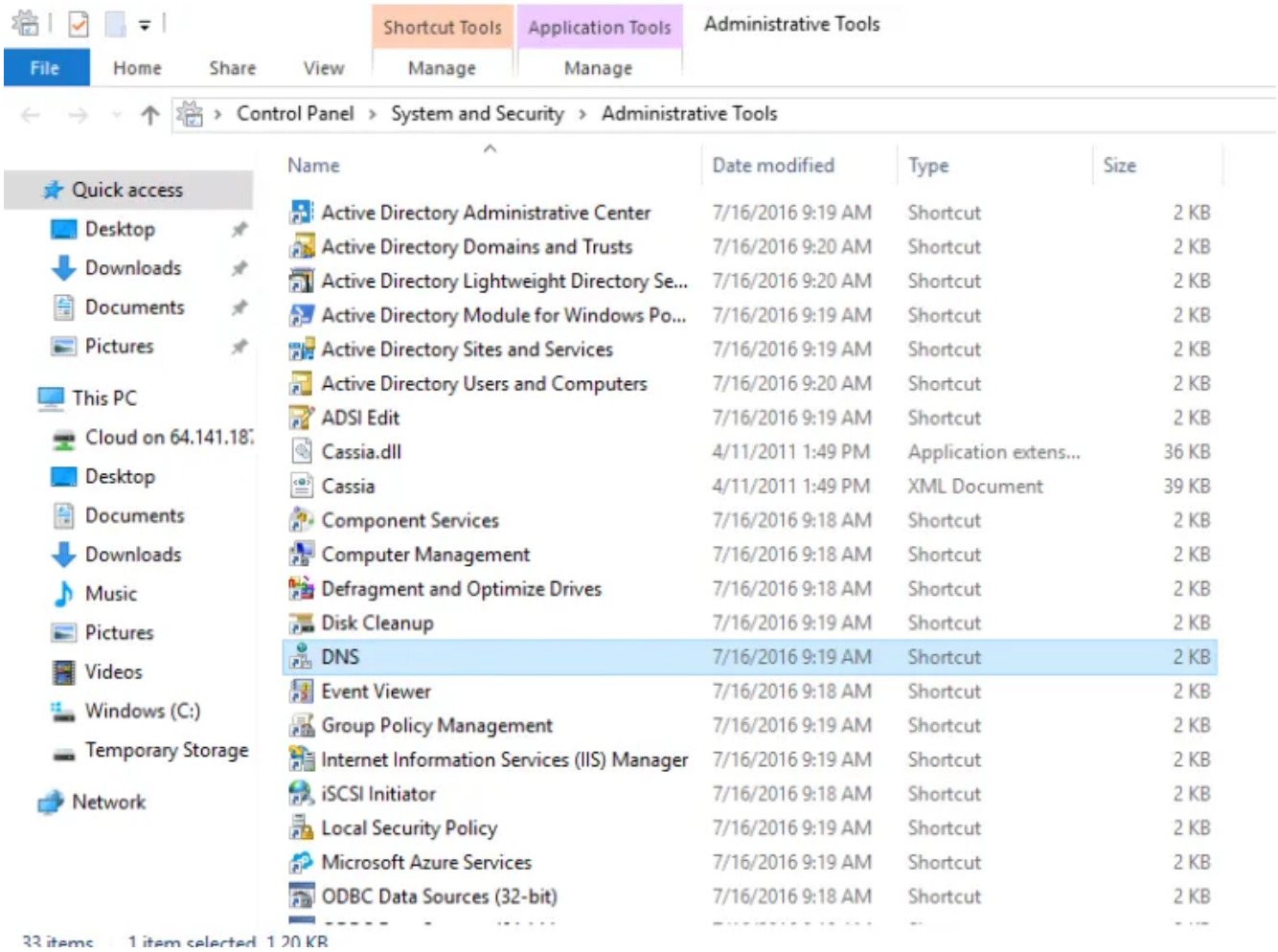

Add Roles and Features Wizard
Before you begin
DESTINATION SERVER
contoso100-test.contoso100.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.
To remove roles, role services, or features:
Start the Remove Roles and Features Wizard
Before you continue, verify that the following tasks have been completed:
• The Administrator account has a strong password
• Network settings, such as static IP addresses, are configured
• The most current security updates from Windows Update are installed
If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.
To continue, click Next.
Skip this page by default
< Previous
Next >
Install
Cancel


Add Roles and Features Wizard
Select installation type
DESTINATION SERVER
contoso100-test.contoso100.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).
Role-based or feature-based installation
Configure a single server by adding roles, role services, and features.
Remote Desktop Services installation
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.
< Previous
Next >
Install
Cancel


Add Roles and Features Wizard
Select destination server
DESTINATION SERVER
cwmgr1.cloudjumper.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select a server or a virtual hard disk on which to install roles and features.
Select a server from the server pool
Select a virtual hard disk
Server Pool
Filter:
Name
IP Address
Operating System
cwmgr1.cloudjumper.com
10.0.0.12
Microsoft Windows Server 2016 Datacenter
1 Computer(s) found
This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.
< Previous
Next >
Install
Cancel



2. Once installed, you can go to Control Panel → System and Security → Administrative Tools and open up DNS.



3. When asked for the DNS server running DNS you will want to put in your domain name (in the example we've been using, this would be *netapp.com*).

Troubleshooting Application Issues

Overview

Troubleshooting an application error is a common administrative practice that doesn't involve VDS itself, but is greatly assisted by VDS and the level of control it provides administrators. While NetApp VDS does not troubleshoot these issues for Customers, our experience allows us to advice administrators after identifying some basic information like the following in order to dig deeper and troubleshoot with end users and/or third parties.

- Name of the user experiencing the issue
- Name of the application the user was working with
- The server the user's session was on
- Steps to reproduce the issue

Reviewing Your Tools

Monitoring

After identifying the server the User was using, check your monitoring solution to validate that resource (CPU and RAM) consumption is within normal levels. You can also validate that application-specific requirements (a special service that will cause issues if it isn't running) are functional. In situations like this, advanced settings like up/down monitoring of said services may have been triggered.

Anti-Virus

As an administrator with access to both the servers and Azure Active Directory, you have access to review what has been discovered and what policies are set. In the event something unforeseen is present, it could be affecting your application.

Additional Tools

Some applications require additional components, like a service account that remains logged in indefinitely or a VPN to a piece of physical equipment (say, an on-site network appliance or a piece of manufacturing equipment or diagnostic utility). In these situations, application-specific errors may be caused by something other than the way the application was installed or how its settings are configured.

Extending Access to Third Parties

Applications and/or their databases are often installed, configured and supported by either the software vendor (ISV) themselves or a third party expert in that software's configuration, management and integrations. In these situations you will want to extend temporary administrative access to a these steps: Providing Temporary Access to 3rd Parties

It is a best practice to shut down these third party accounts after the upgrade or update is completed or after the issue is resolved.

In many cases, this level of troubleshooting will require that a software maintenance contract with the ISV. If this is not in place, the ISV may not assist you until this is in place.

It is also possible that the troubleshooting issue could be related to the hardware (desktops, laptops, thin clients, etc.) end users are working with. An example could be that upgrading a user's laptop could lock the machine in the eyes of a thin client configuration file, meaning that end users cannot access the tools that allow them to log into their virtual desktop. In this case, a maintenance contract for hardware may be required before the manufacturer will assist you.