Microsoft

Desktop-as-a-Service (DaaS) using Windows Virtual Desktop (WVD)

Diagnostics Service & Troubleshooting

Prepared for
Service Providers
Oct, 2019

Prepared by
Microsoft – **O**ne **C**ommercial **P**artner (OCP)

MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Contents

1. Overview

Windows Virtual Desktop Preview offers a diagnostic feature that allows the administrator to identify issues through a single interface. The Windows Virtual Desktop roles log a diagnostic activity whenever a user interacts with the system. Each log contains information such as error messages, tenant information, and user information.

This guide illustrates the steps for diagnosing connection and operational errors within the new Windows Virtual Desktop (WVD) Service in Microsoft Azure.

Please be advised this information is provided to help understand/summarize this process and your enterprises` implementation may contain additional customizations and/or settings that ***might not*** be covered in this document.

2. Prerequisites

Azure & Windows Active Directory Prerequisites

Before getting started, **all** items listed below **must** be checked/validated to ensure the most basic requirements are in place to proceed with executing the remaining steps in this guide.

- A working Windows Virtual Desktop environment
- Windows Virtual Desktop PowerShell module installed on the work station
- An HTML5 compatible browser installed on the work station. Most modern browsers are HTML5 compatible.

General Best Practices

Since everyone's business and technical requirements vary across the board, it is always a good idea to familiarize yourselves with the standard best practices across the different Azure technologies & services.

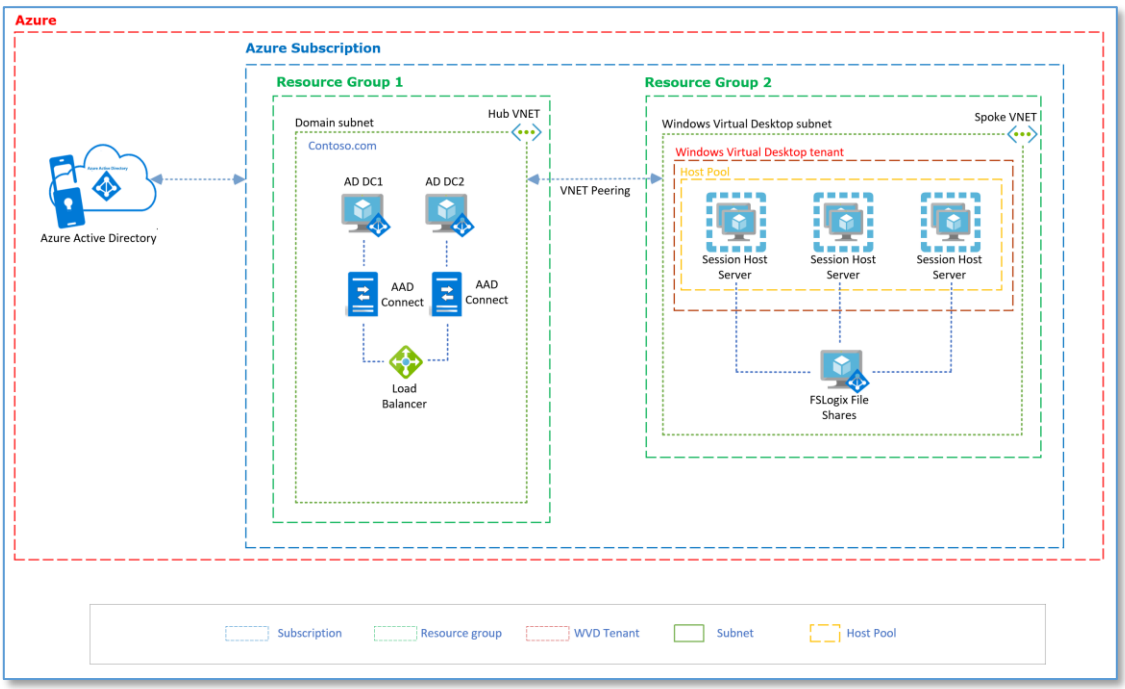
- Please follow the guidance here to maintain a consistent naming convention across your resources, unless you are already using a naming system.
- Azure security best practices and patterns
- Azure Active Directory Hybrid Identity best practices
- Azure identity management and access control security best practices
- Azure Networking & security Best Practices
- Azure Storage security overview
- Best practices for Azure VM security

Azure Networking

The recommendation is to design your Azure Networking using a Hub-Spoke topology. Consider the HUB like a DMZ deployed with your Virtual network Gateways and other security/edge appliances like Firewalls Etc. while the Spoke will act as the backend zone where your session hosts servers are deployed to and is peered with the HUB. This is our design for this walk-through, so you'll need this already setup before proceeding.

Azure Architectural Diagram

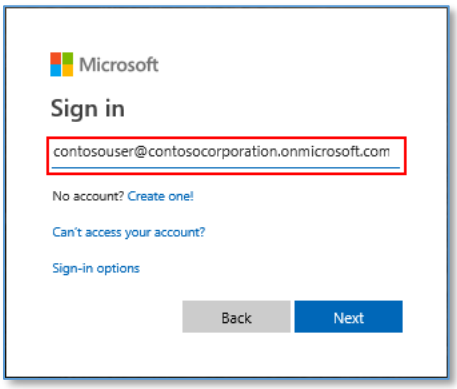
Below is a diagram of the Azure environment that we'll use. It shows the objects created in Azure and their relationships within the environment. In this example, the company name will be Contoso.



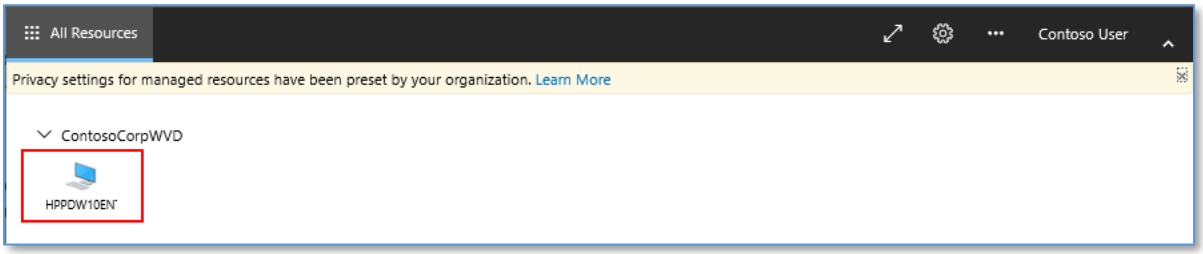
3. Identifying WVD logon errors with a browser

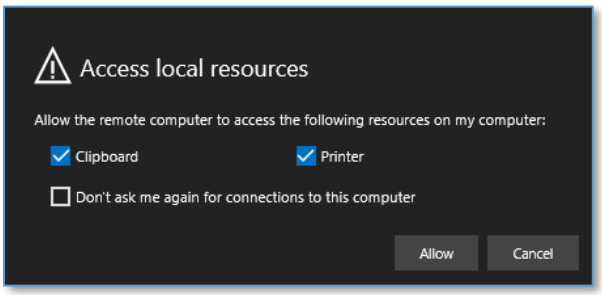
Accessing your WVD tenant through a browser enables you to capture detailed diagnostic information during the logon process. In this section, we'll show how logging may be turned-on and used to identify errors.

1. Using an HTML5 compatible web browser, navigate to your WVD portal and login. In this walk-through, we'll use the default: https://rdweb.wvd.microsoft.com/webclient/index.html

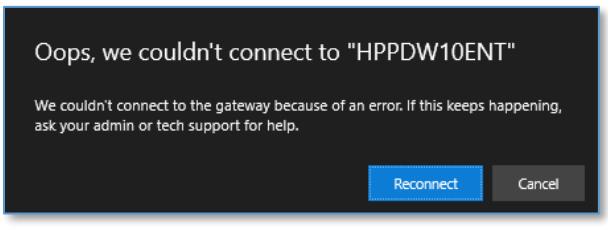


2. Clicking the desktop icon *should* open the desktop as expected:

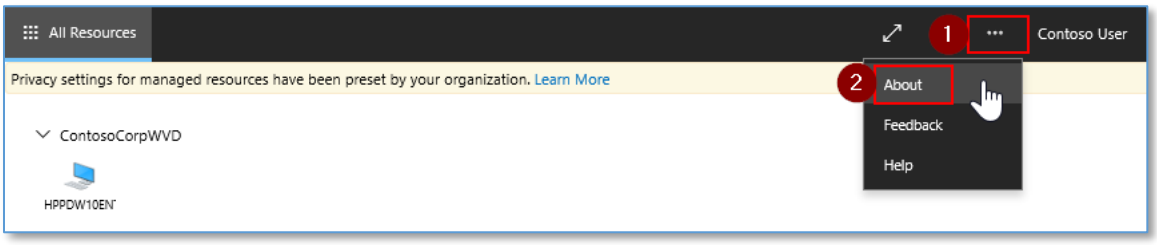




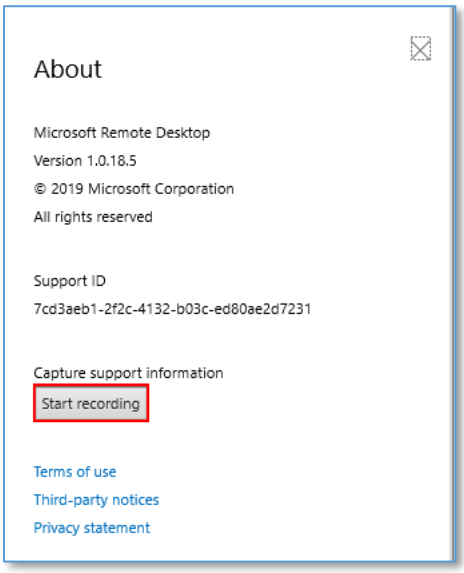
However, in our case, we get an error after clicking **Allow**:



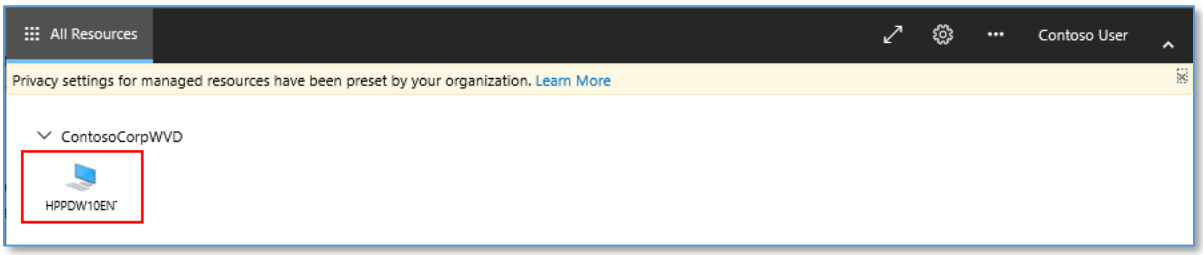
3. Enable the recording tool by clicking the **More Options** icon, then **About**:

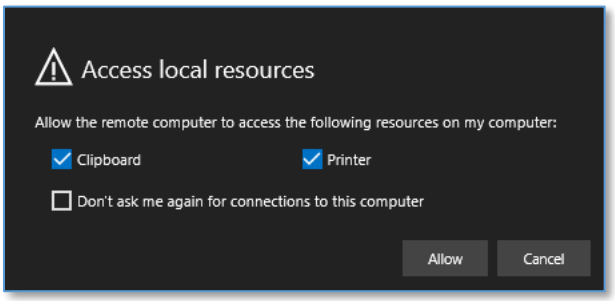


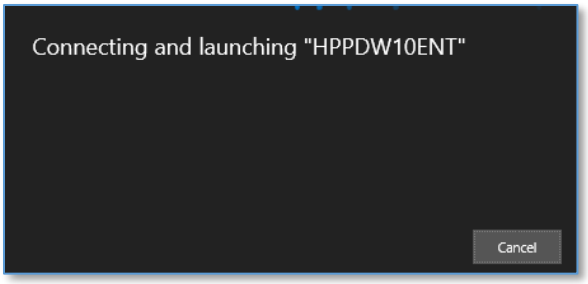
4. Click the Start Recording button:

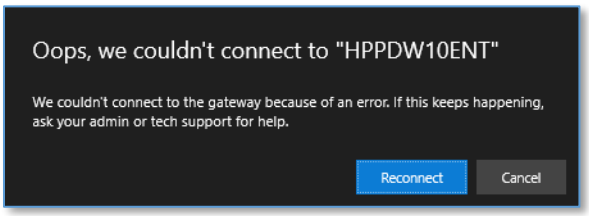


5. Click the desktop icon again:

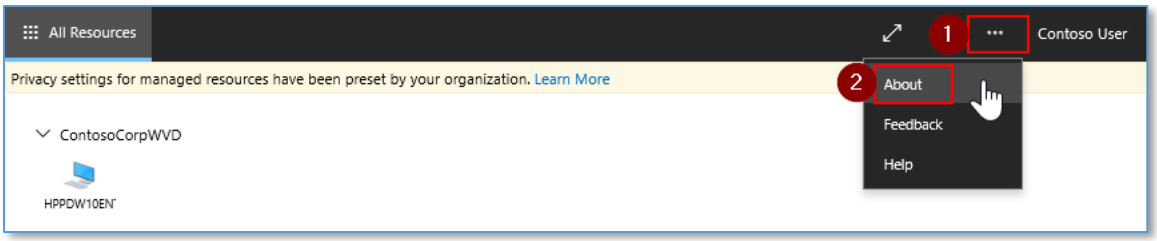


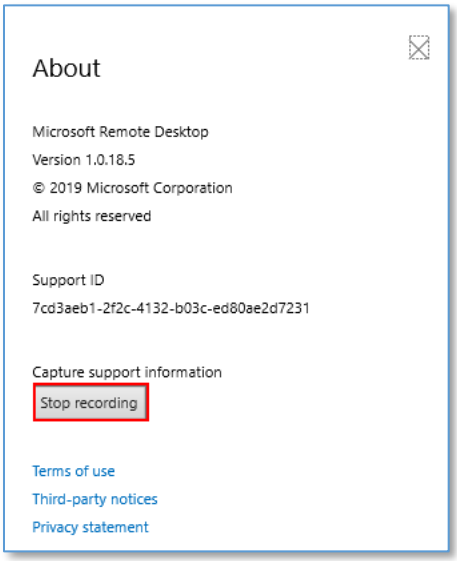




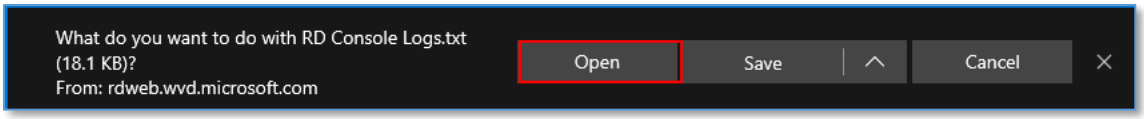


6. Stop the recording tool through the **More Options** icon & **About** again:

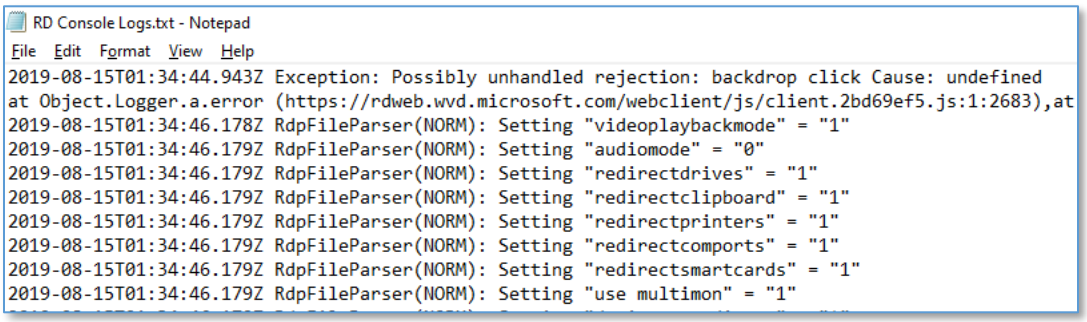




7. **Open** the RD Console Logs.txt file when asked:



...which displays each connection process operation, ordered by time:



8. Look for an error message towards the end of the file. Here's what ours states: *error code: 2147965470 message: Failed to add user = â‰¤contosouser@contosocorporation.onmicrosoft.comâ‰¥ to group = Remote Desktop Users. Reason: Win32.ERROR_NO_SUCH_MEMBER*

9. In this case, *ERROR_NO_SUCH_MEMBER* means that the user attempting to logon was never added to any WVD app groups. Adding the user resolves the problem.

4. Diagnose WVD issues with PowerShell

Windows Virtual Desktop Diagnostics uses just one PowerShell cmdlet but contains many optional parameters to help narrow down and isolate issues. In this section we'll access and view the various diagnostics features.

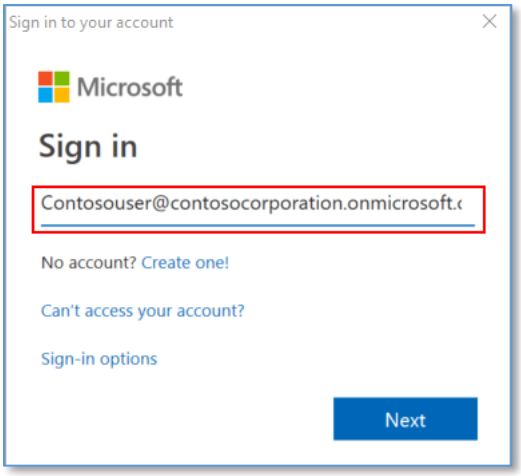
Retrieve diagnostic activities in your tenant

You can retrieve diagnostic activities by using the **Get-RdsDiagnosticActivities** cmdlet. The following example cmdlet will return a list of diagnostic activities, sorted from most to least recent.

From a work station with PowerShell and the Windows Virtual Desktop PowerShell module installed, run the commands below. In our examples, we're using the tenant **ContosoCorpWVD**:

1. Login to the Azure WVD tenant

```
# Import PS module & Logon to the WVD tenant:
Import-Module -Name Microsoft.RDInfra.RDPowerShell
Add-RdsAccount -DeploymentUrl "https://rdbroker.wvd.microsoft.com"
```




```
DeploymentUrl                    TenantGroupName
-------------                    ---------------
https://rdbroker.wvd.microsoft.com Default Tenant Group
```

2. Show any WVD errors:

```
# Get the diagnostics information:
Get-RdsDiagnosticActivities -TenantName "ContosoCorpWVD"
```

```
PS C:\WINDOWS\system32> Get-RdsDiagnosticActivities -TenantName "ContosoCorpWVD"


ActivityId        : 558016c1-7254-4f27-84ed-09b14d7e093e
ActivityType      : Management
StartTime         : 8/14/2019 5:47:08 PM
EndTime           : 8/14/2019 5:47:09 PM
UserName          : contosouser@contosocorporation.onmicrosoft.com
RoleInstances     : mrs-cusr1c001-rdbroker-prod::RD501AC504640D
Outcome           : Success
Status            : Completed
Details           :
LastHeartbeatTime : 8/14/2019 5:47:09 PM
Checkpoints       :
Errors            :
```

That's good news, no errors and **LastHeartBeatTime** is current.

3. Let's create a situation to see the diagnostics feature in action. One way to cause a new diagnostics record, or **Activity**, to be recorded, is by simply ending the WVD session by closing the browser while the user is logged-on. Do this in your own WVD instance, then run the below PowerShell command, using your WVD tenant name:

```
# Get the diagnostics information:
Get-RdsDiagnosticActivities -TenantName "ContosoCorpWVD" -Detailed
```

Ours returns:

```
ActivityId        : aef7f1d9-598a-45e0-b623-15eb320e0000
ActivityType      : Connection
StartTime         : 8/14/2019 6:41:07 PM
EndTime           : 8/14/2019 6:42:43 PM
UserName          : contosouser1@contosocorporation.onmicrosoft.com
RoleInstances     : rdwebclient;mrs-cusr1c001-rdgateway-prod::RD0003FF62ADF3;mrs-cusr1c001-rdbroker-prod::RD0003FF64135F;≤rdshvm-0.contos
                    o.local≥
Outcome           : Failure
Status            : Completed
Details           : {[ClientOS, Win32 Chrome 76.0.3809.100], [ClientVersion, 1.0.18.5], [ClientType, HTML], [PredecessorConnectionId,
                    ]...}
LastHeartbeatTime : 8/14/2019 6:42:44 PM
Checkpoints       : {LoadBalancedNewConnection, TransportConnecting, TransportConnected, RdpStackDisconnect}
Errors            : {Microsoft.RDInfra.Diagnostics.Common.DiagnosticsErrorInfo}
```

We can see that **Outcome = Failure**, but there's really nothing else useful.

View detailed error messages for a failed activity by activity ID

4. Using the **ActivityID** from the error information:

```
ActivityId        : aef7f1d9-598a-45e0-b623-15eb320e0000
ActivityType      : Connection
StartTime         : 8/14/2019 6:41:07 PM
EndTime           : 8/14/2019 6:42:43 PM
UserName          : contosouser1@contosocorporation.onmicrosoft.com
RoleInstances     : rdwebclient;mrs-cusr1c001-rdgateway-prod::RD0003FF62ADF3;mrs-cusr1c001-rdbroker-prod::RD0003FF64135F;≤rdshvm-0.contos
                    o.local≥
Outcome           : Failure
Status            : Completed
Details           : {[ClientOS, Win32 Chrome 76.0.3809.100], [ClientVersion, 1.0.18.5], [ClientType, HTML], [PredecessorConnectionId,
                    ]...}
LastHeartbeatTime : 8/14/2019 6:42:44 PM
Checkpoints       : {LoadBalancedNewConnection, TransportConnecting, TransportConnected, RdpStackDisconnect}
Errors            : {Microsoft.RDInfra.Diagnostics.Common.DiagnosticsErrorInfo}
```

...and adding some additional PowerShell code, we can see more detail:

```
# See errors inner detail using an Activity ID (multiple errors may be listed)
Get-RdsDiagnosticActivities -TenantName "ContosoCorpWVD" `
-ActivityId aef7f1d9-598a-45e0-b623-15eb320e0000 -Detailed `
| Select-Object -ExpandProperty Errors
```

```
PS C:\WINDOWS\system32> Get-RdsDiagnosticActivities -TenantName "ContosoCorpWVD" `
-ActivityId aef7f1d9-598a-45e0-b623-15eb320e0000 -Detailed `
| Select-Object -ExpandProperty Errors


ErrorSource       : Client
ErrorOperation    : ClientRDPConnect
ErrorCode         : 8
ErrorCodeSymbolic : ConnectionBroken
ErrorMessage      : ConnectionBroken
ErrorInternal     : False
ReportedBy        : Client
Time              : 8/14/2019 6:42:43 PM
```

Sure enough, the client was disconnected unexpectedly, or not "cleanly".

Filter diagnostic activities by user

Using the **-UserName** parameter allows us to filter all of the diagnostics information by that users` logon ID. In our example below, we'll locate specific error information for our Contosouser1 user:

```
# Filter errors by user
Get-RdsDiagnosticActivities -TenantName "ContosoCorpWVD" `
-UserName contosouser1@contosocorporation.onmicrosoft.com
```

```
ActivityId        : 0cce3f47-d2ea-4fe1-808b-52297f650000
ActivityType      : Connection
StartTime         : 8/14/2019 8:36:22 PM
EndTime           : 8/14/2019 8:36:45 PM
UserName          : contosouser1@contosocorporation.onmicrosoft.com
RoleInstances     : rdwebclient;mrs-cusr1c002-rdgateway-prod::RD0003FFDC4949;mrs-cusr1c001-rdbroker-prod::RD0003FF62DBF8;≤rdshvm-0.contos
                    o.local≥
Outcome           : Failure
Status            : Completed
Details           :
LastHeartbeatTime : 8/14/2019 8:36:45 PM
Checkpoints       :
Errors            :
```

Using the **ActivityID** above, and the PS code from earlier, let's see the detailed error information:

```
# See errors inner detail using an Activity ID (multiple errors may be listed)
Get-RdsDiagnosticActivities -TenantName "ContosoCorpWVD" `
-ActivityId 0cce3f47-d2ea-4fe1-808b-52297f650000 -Detailed `
| Select-Object -ExpandProperty Errors
```

```
PS C:\WINDOWS\system32> # See errors inner detail using an Activity ID (multiple errors may be listed)
Get-RdsDiagnosticActivities -TenantName "ContosoCorpWVD" `
-ActivityId 0cce3f47-d2ea-4fe1-808b-52297f650000 -Detailed `
| Select-Object -ExpandProperty Errors


ErrorSource       : RDStack
ErrorOperation    : ConnectionEstablished
ErrorCode         : 14
ErrorCodeSymbolic : UnexpectedNetworkDisconnect
ErrorMessage      : Unexpected network disconnect
ErrorInternal     : False
ReportedBy        : RDStack
Time              : 8/14/2019 8:36:45 PM
```

Once again, we can see that the client was disconnected unexpectedly.

Filter diagnostic activities by date

You can filter the returned diagnostic activity list with the -**StartTime** and -**EndTime** parameters. The -StartTime parameter used alone, will return a diagnostic activity list starting from a specific date, as shown in the following example.

```
# Filter activities by date
Get-RdsDiagnosticActivities -TenantName "ContosoCorpWVD" -StartTime "08/14/2019"
```

```
ActivityId        : 01b9f43c-c4d1-49fb-8095-46d9b9800000
ActivityType      : Connection
StartTime         : 8/14/2019 6:34:09 PM
EndTime           : 8/14/2019 6:34:14 PM
UserName          : contosouser@contosocorporation.onmicrosoft.com
RoleInstances     : rdwebclient;mrs-cusr1c002-rdgateway-prod::RD0003FFDC4949;≤rdshvm-1.contoso.local≥;mrs
                    FF646C43
Outcome           : Failure
Status            : Completed
Details           :
LastHeartbeatTime : 8/14/2019 6:35:46 PM
Checkpoints       :
Errors            :

ActivityId        : 7e76bec1-f23b-481a-9d9a-7f40e0290000
ActivityType      : Connection
StartTime         : 8/14/2019 6:31:20 PM
EndTime           : 8/14/2019 6:31:27 PM
UserName          : contosouser@contosocorporation.onmicrosoft.com
RoleInstances     : rdwebclient;mrs-cusr1c002-rdgateway-prod::RD0003FFDC4949;mrs-cusr1c002-rdbroker-prod:
                    o.local≥
Outcome           : Failure
Status            : Completed
Details           :
LastHeartbeatTime : 8/14/2019 6:32:57 PM
Checkpoints       :
Errors            :

ActivityId        : 61787e6e-196c-46b2-9ff6-275d3d9740cf
ActivityType      : Feed
StartTime         : 8/14/2019 6:30:11 PM
EndTime           : 8/14/2019 6:30:12 PM
UserName          : contosouser@contosocorporation.onmicrosoft.com
RoleInstances     : rdwebclient;mrs-cusr0c002-rdbroker-prod::RD2818789AE617
Outcome           : Success
Status            : Completed
Details           :
LastHeartbeatTime : 8/14/2019 6:30:12 PM
Checkpoints       :
Errors            :

ActivityId        : 558016c1-7254-4f27-84ed-09b14d7e093e
ActivityType      : Management
StartTime         : 8/14/2019 5:47:08 PM
EndTime           : 8/14/2019 5:47:09 PM
UserName          : contosouser@contosocorporation.onmicrosoft.com
RoleInstances     : mrs-cusr1c001-rdbroker-prod::RD501AC504640D
Outcome           : Success
Status            : Completed
Details           :
LastHeartbeatTime : 8/14/2019 5:47:09 PM
Checkpoints       :
Errors            :
```

… and on and on.

Add the -**EndTime** parameter to limit the returned list size:

```
# Filter activities by date
Get-RdsDiagnosticActivities -TenantName "ContosoCorpWVD" `
-StartTime "8/14/2019 5:47:08 PM" -EndTime "8/14/2019 6:32:00 PM"
```

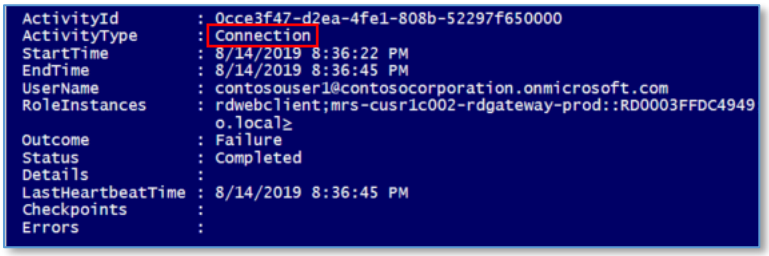
```
ActivityId        : 7e76bec1-f23b-481a-9d9a-7f40e0290000
ActivityType      : Connection
StartTime         : 8/14/2019 6:31:20 PM
EndTime           : 8/14/2019 6:31:27 PM
UserName          : contosouser@contosocorporation.onmicrosoft.com
RoleInstances     : rdwebclient;mrs-cusr1c002-rdgateway-prod::RD0003FFDC4949;m
                    o.local≥
Outcome           : Failure
Status            : Completed
Details           :
LastHeartbeatTime : 8/14/2019 6:32:57 PM
Checkpoints       :
Errors            :

ActivityId        : 61787e6e-196c-46b2-9ff6-275d3d9740cf
ActivityType      : Feed
StartTime         : 8/14/2019 6:30:11 PM
EndTime           : 8/14/2019 6:30:12 PM
UserName          : contosouser@contosocorporation.onmicrosoft.com
RoleInstances     : rdwebclient;mrs-cusr0c002-rdbroker-prod::RD2818789AE617
Outcome           : Success
Status            : Completed
Details           :
LastHeartbeatTime : 8/14/2019 6:30:12 PM
Checkpoints       :
Errors            :

ActivityId        : 558016c1-7254-4f27-84ed-09b14d7e093e
ActivityType      : Management
StartTime         : 8/14/2019 5:47:08 PM
EndTime           : 8/14/2019 5:47:09 PM
UserName          : contosouser@contosocorporation.onmicrosoft.com
RoleInstances     : mrs-cusr1c001-rdbroker-prod::RD501AC504640D
Outcome           : Success
Status            : Completed
Details           :
LastHeartbeatTime : 8/14/2019 5:47:09 PM
Checkpoints       :
Errors            :
```

This time, the returned list is limited to the 3 records we're interested in.

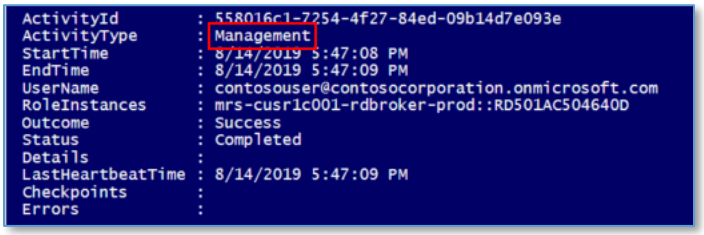
Filter diagnostic activities by activity type

Using the -**ActivityType** parameter, we can see Connection and Management related activities:

```
# Filter activities by Connection ActivityType
Get-RdsDiagnosticActivities -TenantName "ContosoCorpWVD" `
-ActivityType Connection
```



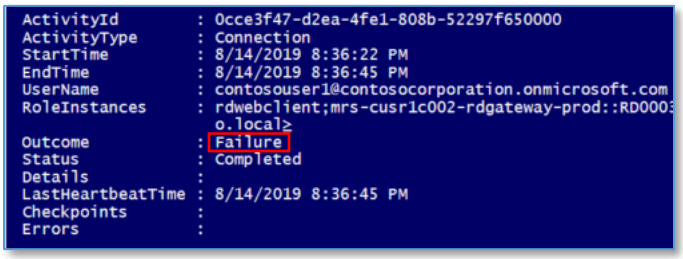

```
# Filter activities by Management ActivityType
Get-RdsDiagnosticActivities -TenantName "ContosoCorpWVD" `
-ActivityType Management
```



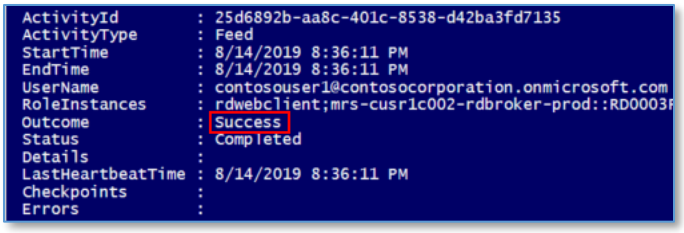
Filter diagnostic activities by outcome

Use the -**Outcome** parameter to find diagnostic activities that were either successful or have failed:

```
# Filter activities by failed Outcome
Get-RdsDiagnosticActivities -TenantName "ContosoCorpWVD" `
-Outcome Failure
```




```
# Filter activities by successful Outcome
Get-RdsDiagnosticActivities -TenantName "ContosoCorpWVD" `
-Outcome Success
```



The -**Outcome** parameter can also be combined with other optional filtering parameters.

5. Appendix

6. Additional Resources

- WVD diagnostic error codes

7. Support

For support queries, please refer to our support portal where you can submit tickets to get additional assistance.