Tutorials

Virtual Desktop Managed Service

NetApp
June 16, 2021

This PDF was generated from https://docs.netapp.com/us-en/virtual-desktop-managed-service/applications.installapplications.html on June 16, 2021. Always check docs.netapp.com for the latest.

Table of Contents

Tutorials . . . 1
- Installing applications on the session host virtual machine(s) . . . 1
- Update and Deploy VM Images . . . 2
- Assigning Users to App Groups . . . 5
- Generate Domain Admin Credentials in VDMS . . . 6

Tutorials

Installing applications on the session host virtual machine(s)

Application Delivery Methodology

Users can access any applications that are installed the session host virtual machine (SHVM) where their user session is running.

Users are assigned to a pool of SHVMs ("host pool") based on their membership in a user group. Every SHVM in that host pool is based on the same VM Image, has the same applications and runs on the same VM resources. Each time a user connects, they are assigned to SHVM in their host pool with the fewest current user sessions.

By adding or removing applications from each SHVM in the host pool the VDMS administrator can control which applications VDMS users can access.

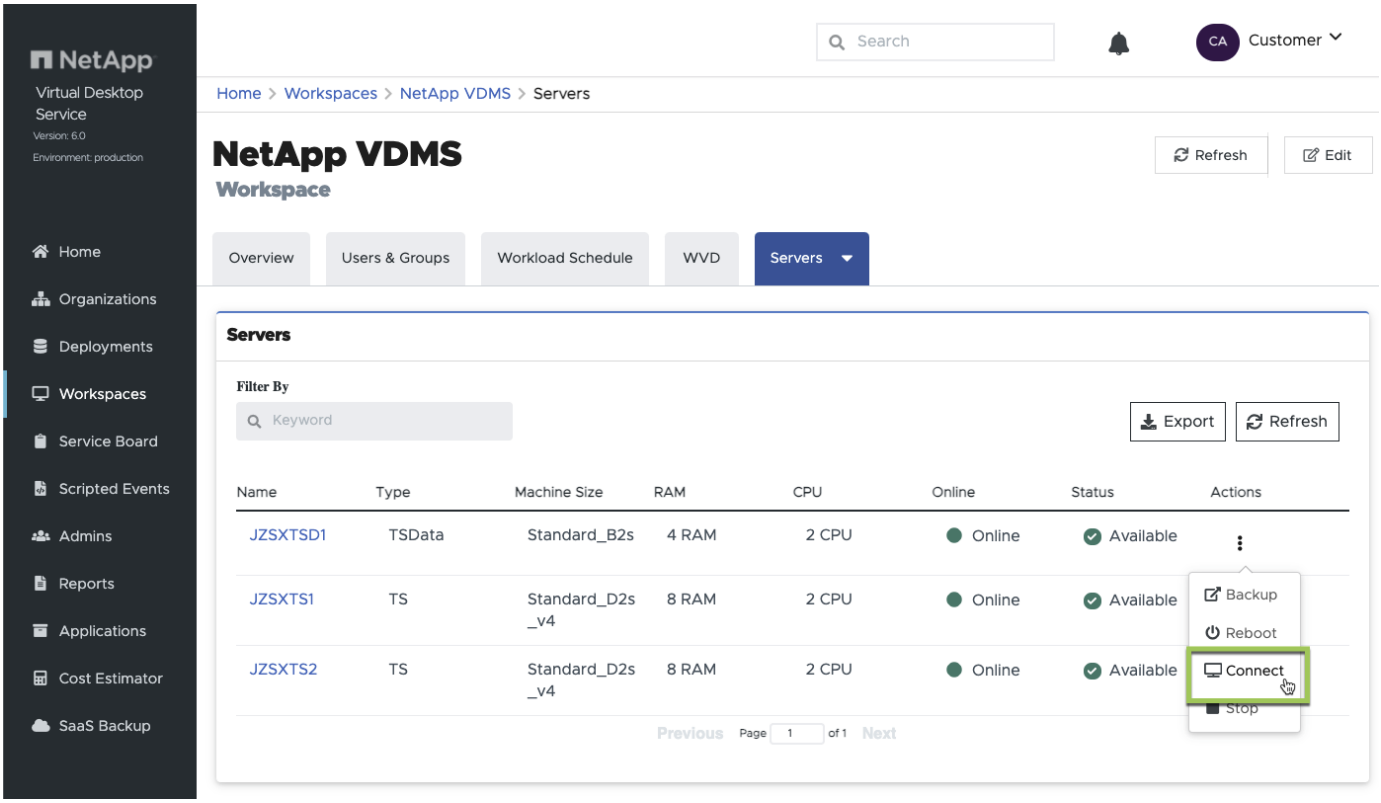
Adding (or removing) applications from each SHVM can be performed directly on each SHVM or to a single VM Image which in turn can be deployed to all SHVMs in the host pool.

This article covers directly installing applications on the SHVMs. VM Image management is covered in this article.

Manual Access

The VDMS management portal provides direct access to each VM via a just-in-time local admin account for all SHVMs and business servers. This access can be used to manually connect to each VM to manually install applications and make other configuration changes.

This functionality is found in Workspace > Servers > Actions > Connect



If domain admin credentials are required, VDMS privileged access management (PAM) functionality to generate domain admin credentials. Details can be found here.

VDMS Automation

With the VDMS portal, the "Scripted Events" section includes functionality to remotely run code.

Within Scripted Events, the Repository tab contains "global" scripts that are published by NetApp. Custom scripts can be added using the "+ Add Script" button.

Within Scripted Events, the Activities tab contains the trigger that causes a script to run against a set of VMs. For VDMS, the "Manual" and "Scheduled" event types are best to push a script across the appropriate virtual machines.

Activities have many available triggers called "Event Types". For VDMS, the "Application Install" and "Application Uninstall" types do not apply. These are RDS-specific triggers and should not be used for VDMS since VDMS is a WVD-based service, and does to follow the design architecture of RDS.

Other Automation Tools

Virtual machines in VDMS can be managed with 3rd party management tools. Application changes and other VM configuration changes can be applied via any compatible tools.

Update and Deploy VM Images

Application Delivery Methodology

Users can access any applications that are installed the session host virtual machine (SHVM) where their user session is running.

Users are assigned to a pool of SHVMs ("host pool") based on their membership in a user group. Every SHVM in that host pool is based on the same VM Image, has the same applications and runs on the same VM resources. Each time a user connects, they are assigned to SHVM in their host pool with the fewest current user sessions.

By adding or removing applications from each SHVM in the host pool the VDMS administrator can control which applications VDMS users can access.

Adding (or removing) applications from each SHVM can be performed directly on each SHVM or to a single VM Image which in turn can be deployed to all SHVMs in the host pool.

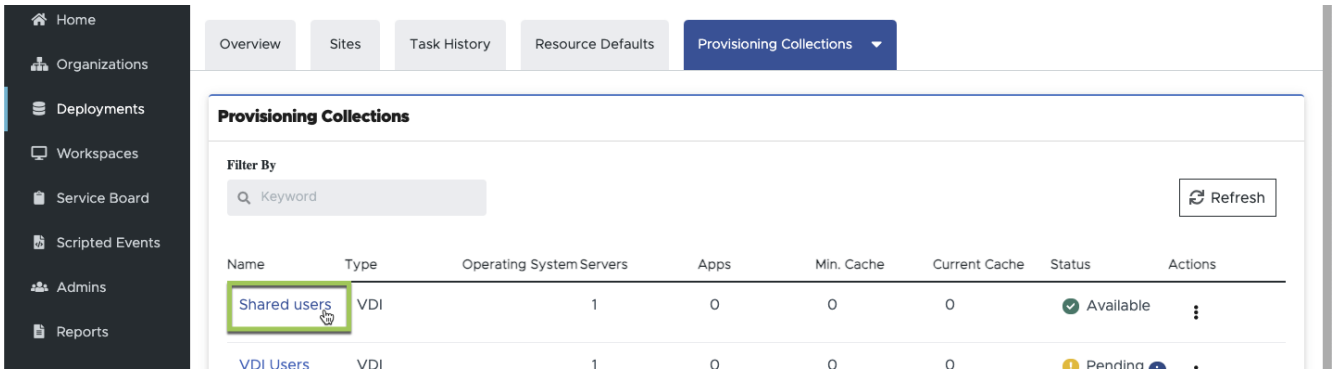
This article covers VM Image management. Directly installing applications on the SHVMs is covered in this article.

Updating the VM Image

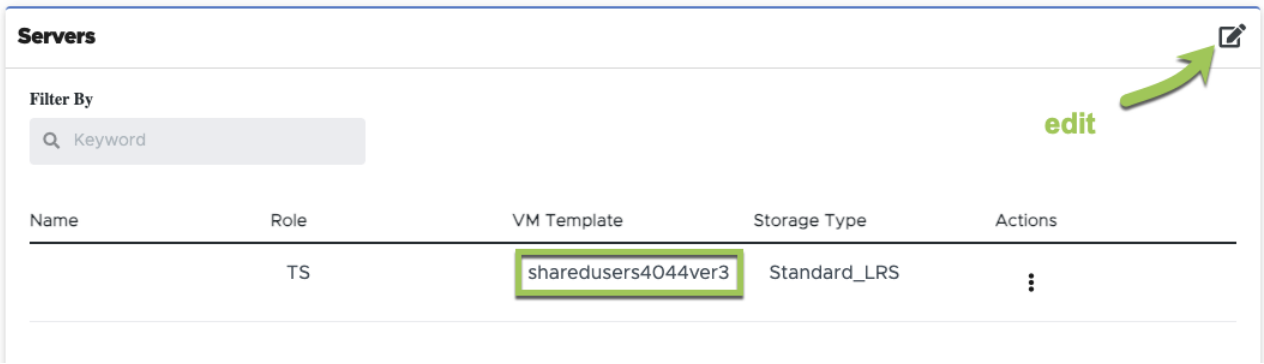
The recommended method for adding (or removing) applications to SHVM(s) is by editing the VM Image assigned to the host pool. Once the VM Image is customized and validated, the VDMS support team can deploy it to all SHVMs in the host pool upon request.

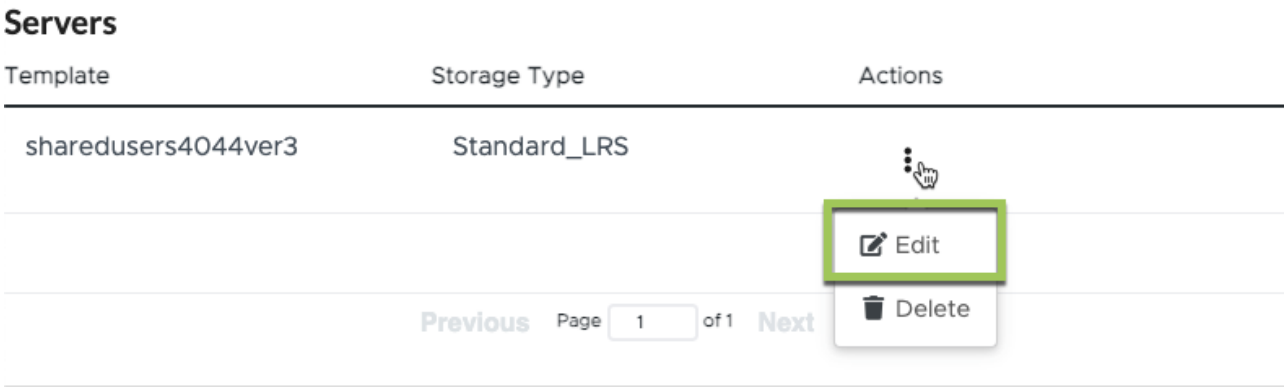
How to edit the VM image

1. Navigate "Provisioning Collections" within the deployment in the VDS portal
2. Click on the provisioning collection associated with the host pool you wish to update.

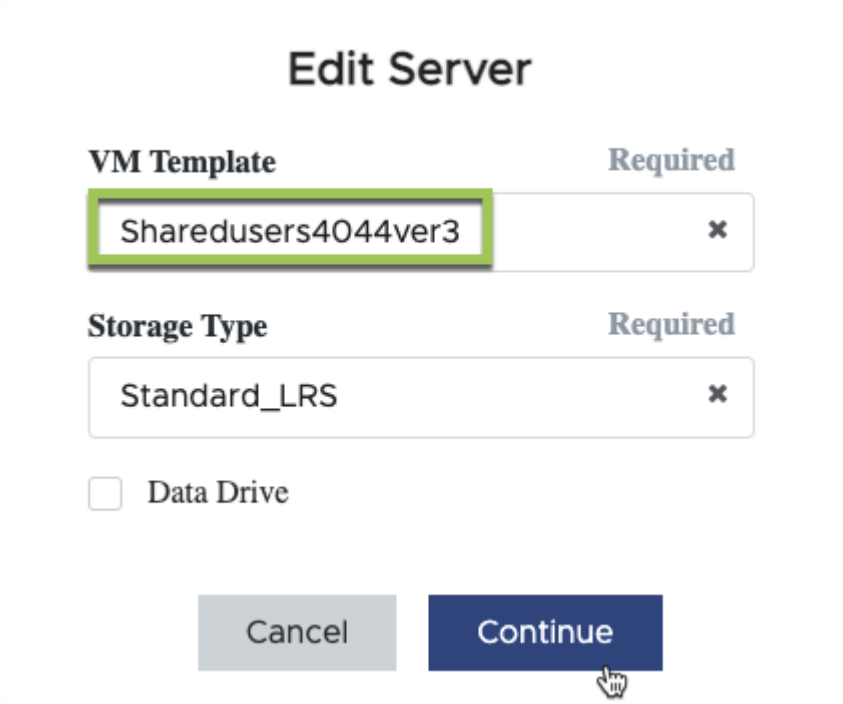


a. Make note of the "VM Template" name in the "Servers section.





3. Edit the Server template ensuring that the source template is the VM Template noted in step 2.a. above. Click "Continue"



Don’t edit these settings:
1. Type = VDI
2. Share Drive = empty
3. Minimum Cache = 0
4. Data Drive = Unchecked
5. Storage Type = Standard_LRS

1. The VDMS automation will now build a temporary VM in Azure, the machine name will be *CWT#*. Building this VM may take 25 minutes. Once the process completes the status will change to "Pending"
   a. Note, this VM will run until the customization process is complete so it is important to build, customize and validate the VM within a day or two.
2. Once the temporary VM is ready, you can log on to the VM by editing the Provisioning Collection and then clicking "Connect" on the server.
   a. When prompted for credentials, domain admin credentials can be generated by any VDMS admin with "PAM Approver" rights.

How to deploy an updated VM image

1. Once the VM image is validated, contact the VDMS support team to schedule an image refresh.
2. The team will build new session hosts based on the new image.
    a. If required, please coordinate time to test the new hosts before we redirect new users to the new hosts.
3. Once ready, the support team will redirect all new user sessions to the new hosts. We'll shut down the old hosts once no users are connected. These old VMs will remain in a deallocated state for warm failover but these VMs will be automatically purged after 7 days.

Changing the SHVM(s) directly

Changes can be made directly on the SHVM(s) manually or via any available automation tools. More information on this is found in this article.

When making changes directly to the SHVMs in a host pool it is critical that each SHVM remain configured in the same way or users may have inconsistent experiences as they connect to different SHVMs.

By default, individual SHVMs are not backed up because they typically don't have unique data and are based on a standardized VM image. If you're making customizations directly to the SHVMs, please contact support to get a backup policy applied to one of the SHVMs in the host pool.

Sysprep Troubleshooting

The VDMS image "Validate" function uses Microsoft's Sysprep utility. When validation fails, the most common culprit is a Sysprep failure. To troubleshoot failures, start in the Sysprep log file located on the CWT# VM in the path: C:\windows\system32\Sysprep\panther\setupact.log

Assigning Users to App Groups

User Assignment Methodology

Users are assigned to a session host virtual machine (SHVM) through AD security groups.

For each host pool, there is a linked user group on the "Users & Groups" tab within the workspace.

User groups are named with the workspace ID (a unique 3-4 digit code for each workspace), followed by the name of the host pool.

For example, the group "jzsx Shared Users" is linked to the Shared Users host pool in VDMS. All users added to "jzsx Shared Users" will be assigned access to the session hosts in the "Shared Users" host pool.

To assign a user to their host pool

1. Navigate to "Users & Groups" within the workspace
2. Users can be added to the group by editing the user list within the group.
3. Automation will automatically sync the members of the user group such that the user will be granted access to the appropriate host pool, app group and applications.

Users should only be assigned to one (and only one) app group. The type of host pool (Shared, VDI or GPU) must match the licensed SKUs purchased for VDMS. Misalignment of users and/or assignment to multiple app groups will cause resource contention issues and potentially impact their colleagues working in the environment.

Generate Domain Admin Credentials in VDMS

Privileged Access Management

VDMS admins can be given the "PAM Approver" role which enables the admin to grant PAM requests.

PAM requests will generate a domain level admin account to be used to authenticate on VDMS VMs when the just-in-time local admin credentials are not sufficient.

Any VDMS admin can submit a PAM request but only admins with the PAM Approver role can approve the requests. A PAM Approver can both request and approve their own request.

Submit a PAM Request

To submit a PAM request

1. Navigate to your admin username in the upper right corner and click "Settings"
2. Select the "PAM Requests" tab
3. Click "+ Add"
    a. Select a duration, after which these credentials will expire
    b. Choose the deployment
    c. Enter an email address that the credentials can be provided. This can be any email address, allowing 3rd parties (e.g. a vendor) to be granted domain credentials.
    d. Enter a phone number that can receive text messages
    e. Enter any notes for the logs and for the PAM Approver to review.
4. Click "Add Request"

Approve a PAM Request

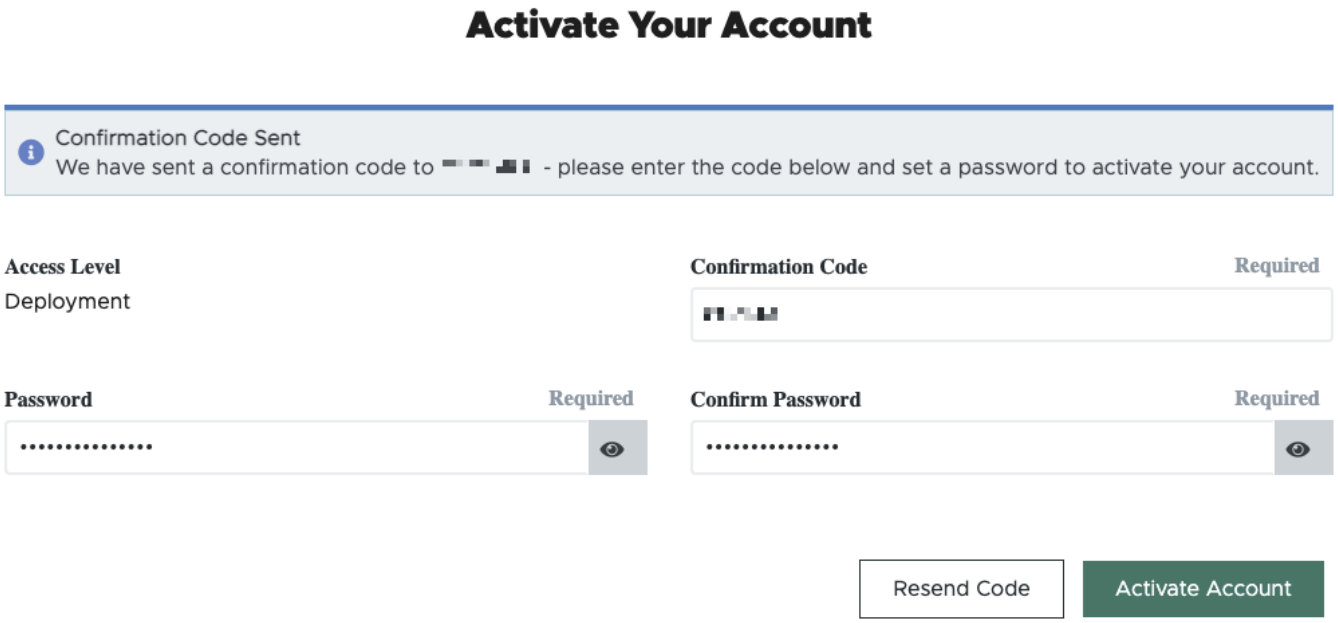
To review and approve/reject a PAM request

1. . Navigate to your admin username in the upper right corner and click "Settings"
2. Select the "PAM Requests" tab and click on the request
3. Review the request and click "Approve" or "Reject"
4. Enter any notes relevant to the approval/rejection decision

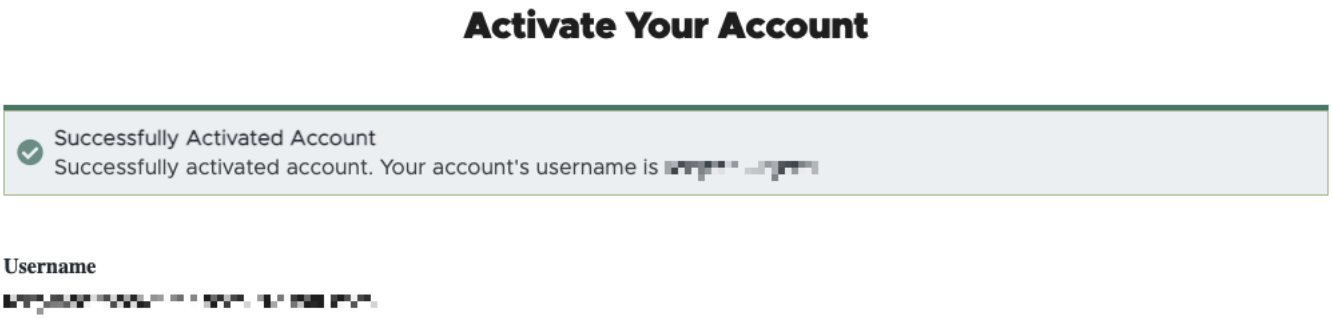
Using PAM Generated Credentials

Once approved, the provided email address is sent a confirmation email to activate their credentials:

Following the "Activate Request" link will bring the user to the following page and send them a confirmation code via SMS. They will also be asked to set a secure password.



Upon successfully validating the account, the user receives a confirmation with their username.



Copyright Information

Copyright © 2021 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.