Technical Report

A Quick Guide to NetApp Data Protection Solutions for Microsoft Office 365

Niyaz Mohamed, NetApp and Roger Yu, AvePoint

May 2016 | TR-4508

TABLE OF CONTENTS

LIST OF FIGURES

 © 2016 NetApp, Inc. All rights reserved.

1 Introduction

This technical report is intended for organizations that want to leverage Microsoft Office 365 software-as-a-service (SaaS) offerings or deploy their messaging and collaboration applications on NetApp® storage in a hybrid topology with Office 365. These organizations want to provide better data management, control, and security and to improve productivity with existing investments.

This document is intended for the following audiences:

- People familiar with the Office 365 solution
- People familiar with Microsoft Exchange Server, SharePoint, and Lync technologies on NetApp private cloud but who want to deploy a hybrid topology with Office 365 functionalities and features

1.1 Statement of Problem

Corporate messaging and collaboration are mission-critical to most organizations. Although it is still early in the adoption phase for cloud-based messaging and collaboration, it has achieved significant traction among organizations of different sizes, industries and geographies. This change in delivery model and priority has imposed additional constraints on IT departments. Small- and medium-sized businesses can take full advantage of Office 365's cloud architecture without having to worry about the complicated integration and migration issues larger enterprises face. In the large enterprise segment, some customers are considering the economics and practicality of the capabilities and risks of moving to Office 365, primarily around the differences between Office 365 and existing systems.

Customers leveraging Office 365 (primarily Exchange Online, SharePoint Online, and OneDrive for Business) want to protect their data and enable recovery if disaster or operational issues occurs.

- Microsoft does not back up Exchange user data. Instead, it protects the Exchange service by creating four copies of each database, which are spread across different data centers.
- Microsoft provides basic functionality to recover from common failures, but it does not replace the need for a backup solution. For example, enhanced database availability group (DAG) capabilities, single-item recovery, and the ability to modify the deleted items retention period from 30 days to unlimited, litigation hold, and inactive mailboxes. However, there are some situations where Office 365 data backups are beneficial because of accidental or intentional data deletion or a misconfiguration in the settings.
- Both SharePoint Online and OneDrive for Business use site and site collection recycle bins that retain deleted data up to 90 days. If the data is manually or automatically deleted from these bins, it is permanently gone. Microsoft, like any other hyperscalar provider, enables backup of its data center. However, Microsoft does not provision backup Exchange data because there are four copies of each database spread across different data centers. In the case of SharePoint, the databases are backed up every 12 hours and are retained for 14 days. However, this capability does not fulfill the requirements of medium-sized to enterprise segments. Although Office 365 offers E3 and E5 plans that provide dumpster and litigation hold capabilities, it is not a complete solution for IT administrators who have always relied on backups.

2 Solution Components

NetApp has partnered with AvePoint to deliver a backup and restore solution for Office 365 that provides NetApp FAS as the target. In addition to the on-premises FAS as the storage option, NetApp provides NetApp AltaVault™ cloud-integrated storage with the NetApp StorageGRID® Webscale system running in a private cloud or cloud service provider premises as another storage repository. This solution provides global deduplication, WAN optimization, and local caching. It also provides automated, daily, full or incremental backups to on-premises FAS controllers, AltaVault physical appliance, or virtual machines (VMs) in the on-premises cloud and provides simple search and restore capabilities including single item.

 © 2016 NetApp, Inc. All rights reserved.

Therefore, customers don't have to risk data loss due to an unexpected purge or some other cause of SaaS data loss, including human error, sync error, malicious insiders, and hacking.

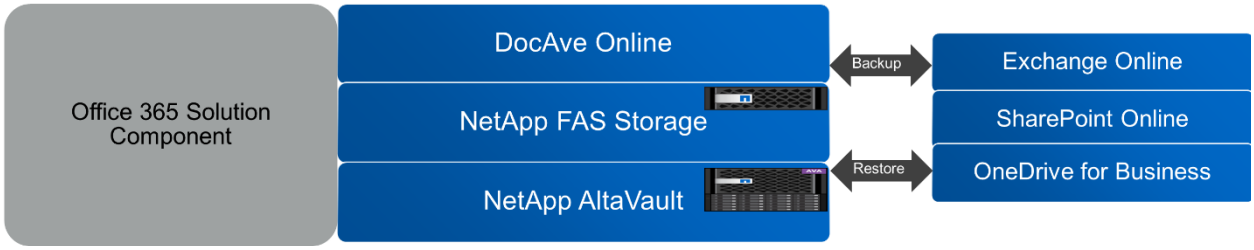
This solution covers Exchange Online; SharePoint Online, including OneDrive for Business at the mailbox, site collection level as well as restores at the mailbox, site collection, and item level.

The following components are included in the solution for Office 365:

- NetApp FAS system
- NetApp AltaVault and StorageGRID Webscale system
- DocAve Online (AvePoint Online Services)

Figure 1 illustrates the integrated AvePoint data protection with high-performance and cloud-enabled NetApp storage and software.

Figure 1) Integrated AvePoint data protection with high-performance and cloud-enabled NetApp storage and software.



2.1 NetApp FAS Array

The NetApp FAS, including NetApp Cloud ONTAP®, addresses the challenges of growing and dynamic businesses. The NetApp storage efficiency features help IT to easily define end-to-end data protection strategies in on-premises and cloud-based deployments. ONTAP® allows users to manage and maintain control of resident cloud data in their terms and offers multiple performance and capacity options for the versatility to meet various storage requirements. NetApp integrated data portability technologies enable dynamic movement of the data among cloud resources and providers. This integration allows quick and granular item-level recovery. The well-known storage efficiency technique provides deduplication level typically ranging between 15% and 30%.

2.2 NetApp AltaVault with StorageGRID Webscale

NetApp AltaVault delivers enterprise-class data protection. AltaVault is an inexpensive solution to storing large numbers of backups, without the cost and maintenance of a secondary data center. AltaVault uses the local disk to store enough data for recovery of most recent backups. This mechanism provides better performance for the most likely restores. The deduplication process uses variable segment length inline deduplication plus compression, which is superior to other techniques such as fixed block. AltaVault deduplication reduces the amount of data stored and typically ranges between 10x and 20x. AltaVault can send data with ease to NetApp StorageGRID Webscale software, giving durable, cost-effective, private cloud archives at web scale. AltaVault offers end-to-end security for data at rest and in flight with the NetApp cryptographic services module.

2.3 DocAve Online

DocAve Online offers powerful backup, administration, and management capabilities through a SaaS platform. Hosted on Microsoft's Azure platform-as-a-service (PaaS) technology, DocAve Online empowers organizations to align cloud computing with their specific business needs. With simplified Office 365 administration, content, and security management, DocAve Online enables organizations to easily extend cloud computing and efficiently respond to evolving business requirements.

 © 2016 NetApp, Inc. All rights reserved.

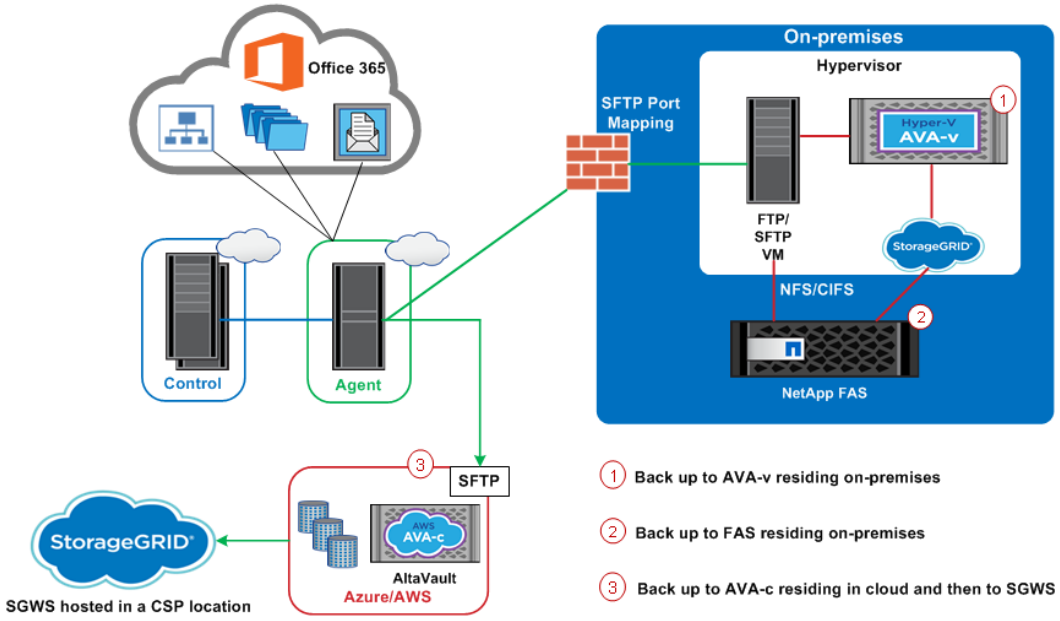
3 Solution Architecture

Many factors can affect the decision to move towards Microsoft Office 365. The rising demand for the availability of a backup and restore solution for Office 365 is inevitable in today's cloud-oriented world. NetApp and DocAve Online together simplify the administration and management of Office 365, as well as provide fast and full-fidelity backup and restore capabilities for SharePoint Online, Exchange Online, and OneDrive for Business. These capabilities also enable organizations to maintain the same level of protection and control over Office 365 assets as is expected with on-premises solutions. DocAve Online uses web services and a CSOM-based SharePoint APIs to back up and restore the data, so there is no need to install or deploy any server side controls.

Backup for Office 365 is a simple and easy-to-use tool that empowers administrators and power users to efficiently back up, archive, and restore their content from Exchange, SharePoint, or OneDrive for Business.

Figure 2 shows Office 365 backup architecture to an on-premises FAS controller or NetApp AltaVault (physical, virtual/cloud).

Figure 2) Office 365 backup architecture to an on-premises FAS controller or NetApp AltaVault (physical, virtual/cloud).

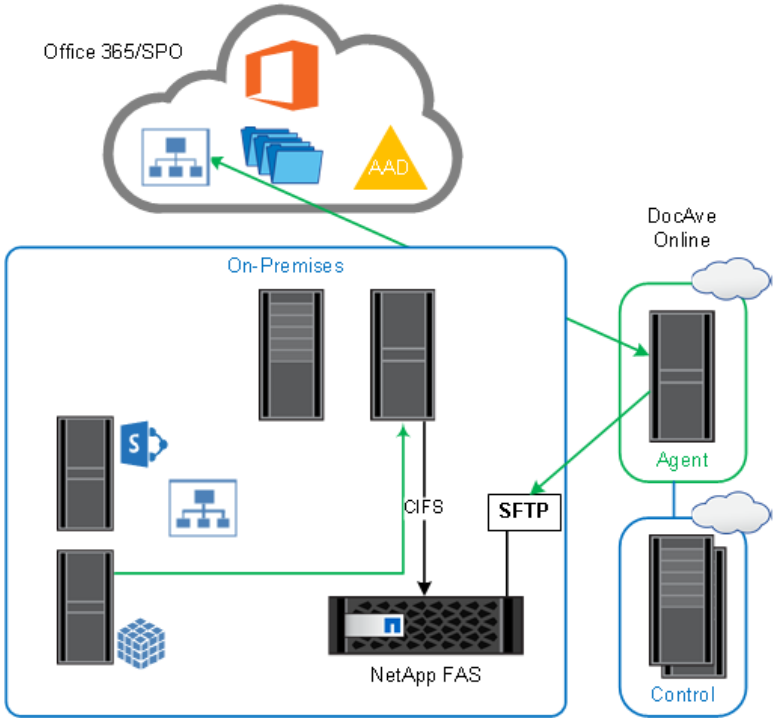


Based on the deployment model and data target criteria, NetApp recommends the following deployment options for storing the backup Office 365 data:

- Option 1: Back up Office 365 data to the FAS controller residing on premises, as shown in Figure 3.

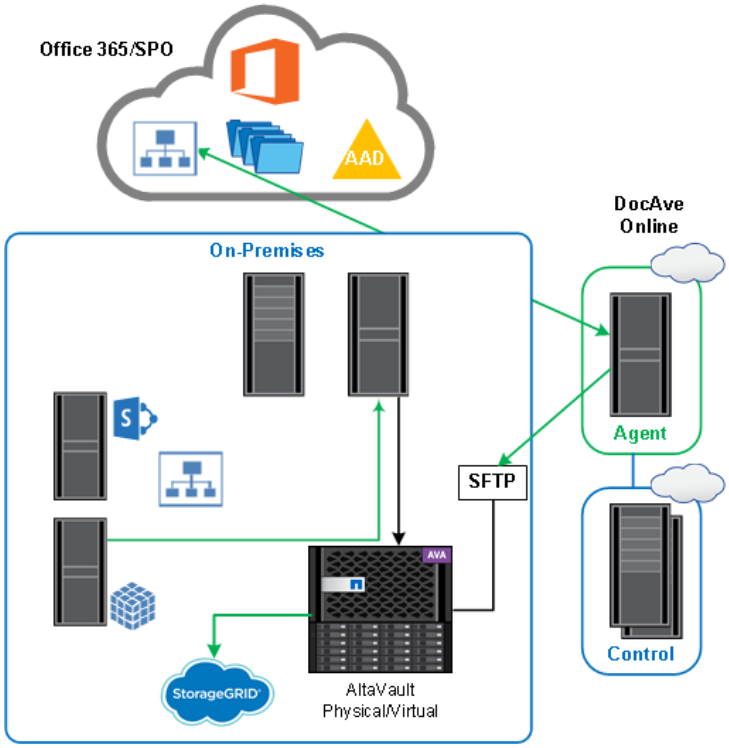
 © 2016 NetApp, Inc. All rights reserved.

Figure 3) Office 365 backup architecture to an on-premises FAS controller.



- Option 2: Back up the Office 365 data to AltaVault residing on premises, as shown in Figure 4.

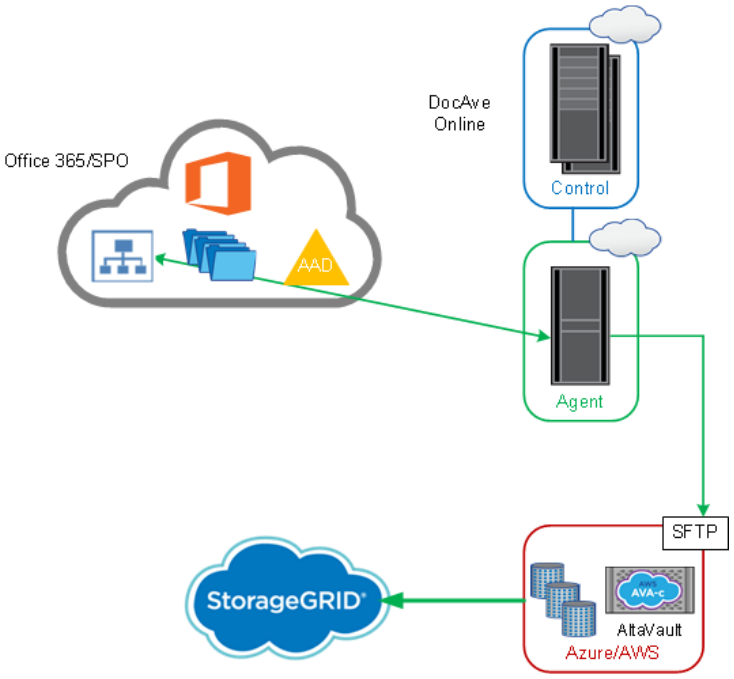
Figure 4) Office 365 backup architecture to NetApp AltaVault residing on premises.



 © 2016 NetApp, Inc. All rights reserved.

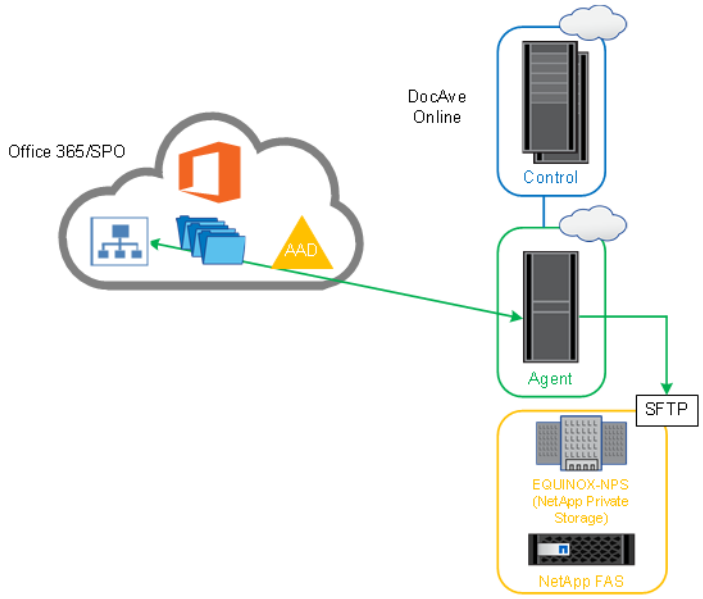
- Option 3: Back up Office 365 data to the AltaVault VM running in the cloud, which provides cloud-to-cloud backup, as shown in Figure 5.

Figure 5) Office 365 backup architecture to NetApp AltaVault residing in the cloud.



- Option 4: Back up Office 365 data to the NetApp private storage (NPS) or AltaVault VM at a co-location facility (such as Equinix), which also provides cloud-to-cloud backup, as shown in Figure 6.

Figure 6) Office 365 backup architecture for NPS FAS controller.



Note: These options apply only to Office 365 deployments and hybrid deployments in which a customer decides to keep the majority percentage of the workload in a NetApp powered private cloud and the remaining percentage of the workload in Office 365. For example, in a hybrid model,

 © 2016 NetApp, Inc. All rights reserved.

customers generally deploy 80% of the workload on premises and 20% of the workload in Office 365.

This document describes the detailed steps to back up Office 365 data using DocAve Online and NetApp values.

4 Back Up and Restore Office 365 Data

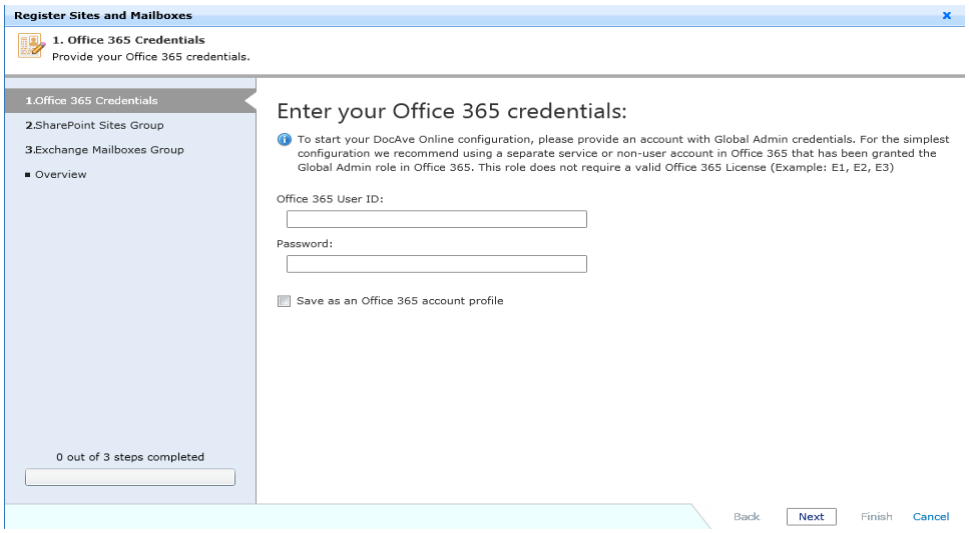
This section describes the steps required to back up and restore Office 365 data hosted in a Microsoft data center.

Register Office 365 Domain

Before performing backup or restore operations, register the site collections and mailboxes. To do this, complete the following steps:

1. Using Internet Explorer browser, navigate to the AvePoint Online Services web site.
2. In the Office 365 Credentials dialog box, enter the Office 365 user ID and password. Click Next.

   Note: To scan all site collections and mailboxes in the specified domain, make sure that the specified Office 365 user ID has the global administrator role. If you are not using a global administrator role, use a SharePoint administrator account in Office 365, navigate to the Control Panel, and scan for site collections in SharePoint Online. Alternatively, using an Exchange administrator account in Office 365, scan for mailboxes in Exchange Online.



3. DocAve Online begins the scan. After the scan completes, the SharePoint Sites Group section is displayed. All of the available site collections are listed under Site Collection in the left pane. Add the desired site collections to the default or customized SharePoint Sites group.

   Note: After this wizard is complete, you can add or reorganize site collections through the DocAve Online Control Panel.

4. Go to the Exchange Mailboxes Group section and scan for the Exchange mailboxes. In the Exchange Mailboxes Group section, all currently available mailboxes are listed under Mailbox in the left pane. You can add mailboxes to the default or customized Exchange Mailboxes group in the right pane.

   Note: After the wizard completes, you can add or reorganize mailboxes through the DocAve Online Control Panel.

5. Review the configuration steps and click Finish to complete the registration.

 © 2016 NetApp, Inc. All rights reserved.

Note: For additional information about content management, control panel, deployment manager, replication, granular backup and restore, and Exchange Online backup and restore functions that are part of DocAve Online, see the DocAve Online 3 User Guide.

Configure Devices and Set Up Storage Policies

In order to perform a backup or restore operation using Exchange Online Backup and Restore or Granular Backup and Restore module, you must first configure one or more physical devices and then set up a storage policy. When performing a backup job, the Exchange Online backup and restore or granular backup and restore module can write to SFTP (a CIFS share exposed using NetApp FAS controller residing on premises) or to NetApp AltaVault residing on premises or in the cloud.

Note: DocAve Online supports specifying a folder in SFTP or NetApp AltaVault to store the data by configuring the folder structure. This field is optional. In the Root Folder text box, enter the desired folder structure in FTP/SFTP/NetApp AltaVault where you would like to store the data (if the specified folder structure does not exist in SFTP/NetApp AltaVault, the folder structure is created automatically). The data is stored according to the specified folder structure. If you do not configure this field, the data is stored in the SFTP/NetApp AltaVault root folder.

Configure SFTP or AltaVault Physical Device

To create a NetApp AltaVault or SFTP physical device, complete the following steps:

1. Navigate to Control Panel > Physical Device.
2. Click Create and then select Physical Device from the drop-down menu to create a physical device. The Create Physical Device or Edit Physical Device interface appears.
3. In the Physical Device Name field, enter a name for the physical device.
4. In the Storage Type field, select NetApp AltaVault/SFTP from the drop-down menu.
5. In the Storage Type Configuration field, configure the following settings:
   - Host
   - Port
   - Root folder
   - User name
   - Password
6. Click Validation Test to verify that the information you entered is correct.
7. Click OK to save the configurations and return to the Storage Configuration interface. After the physical device is saved, it is listed in the Physical Device tab.

Back Up and Restore SharePoint Online (Including OneDrive for Business)

To back up SharePoint Online content, complete the following steps:

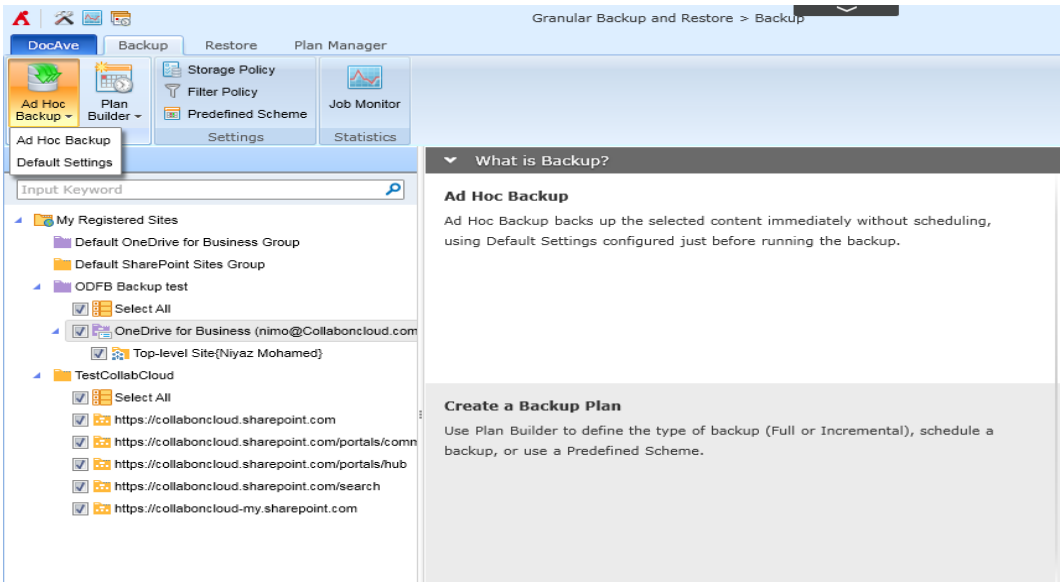
1. Navigate to Granular Backup and Restore > Backup.
2. Expand the Source panel tree to display the objects to be backed up.
3. Select a site's group node and use the Plan Builder to create a plan.

   Note: You can select multiple sites' group nodes to back up, but you cannot select a site's group node and nodes at another level at the same time.

   Note: Site collections or OneDrive for Business sites that were added recently to a site's group are included in an existing plan if the site's group is included in the plan.

   Note: If a SharePoint Online site collection has been deleted, the deleted site collection is backed up or recorded in the backup job report.

 © 2016 NetApp, Inc. All rights reserved.



To restore the granular content at the list/library/folder/item/file level to the designated storage policy, complete the following steps:

1. Navigate to Granular Backup and Restore > Restore.
2. From the Restore tab, select Restore.
3. In the Job Selection interface, select the backup job that contains the granular content that needs to be restored and click Next. The Data Selection interface appears.
4. Expand the Backup Data tree to select the desired SharePoint Online lists/libraries/folders/items/files. Click Next.
5. In the Restore Type interface, select Restore to Storage Policy to restore the selected lists/libraries/folders/items/files.
6. Select a previously created storage policy as the destination to store the restored granular content. Optionally, select New Storage Policy from the drop-down menu to create a new storage policy for the restored granular content.

   Note: Choose to use a single thread or multiple threads during the restore operation using Restore thread file options.

   Note: Granular restore supports skip and overwrite as the apps conflict resolution. It also supports different content-level conflict resolutions such as skip, overwrite, overwrite by last modify time, and append.

Job Monitor

DocAve Online supports the job queue feature to view and manage the jobs waiting in the queue. If the number of running jobs in DocAve Online exceeds the resource limitation, the jobs wait and are displayed in the job queue list. All of the run now jobs and scheduled jobs (when the scheduled time is met) are calculated by the resource limitation. Then the run now jobs and the scheduled jobs designated to execute are added to waiting jobs displaying in the job queue list.

Back Up and Restore Exchange Online

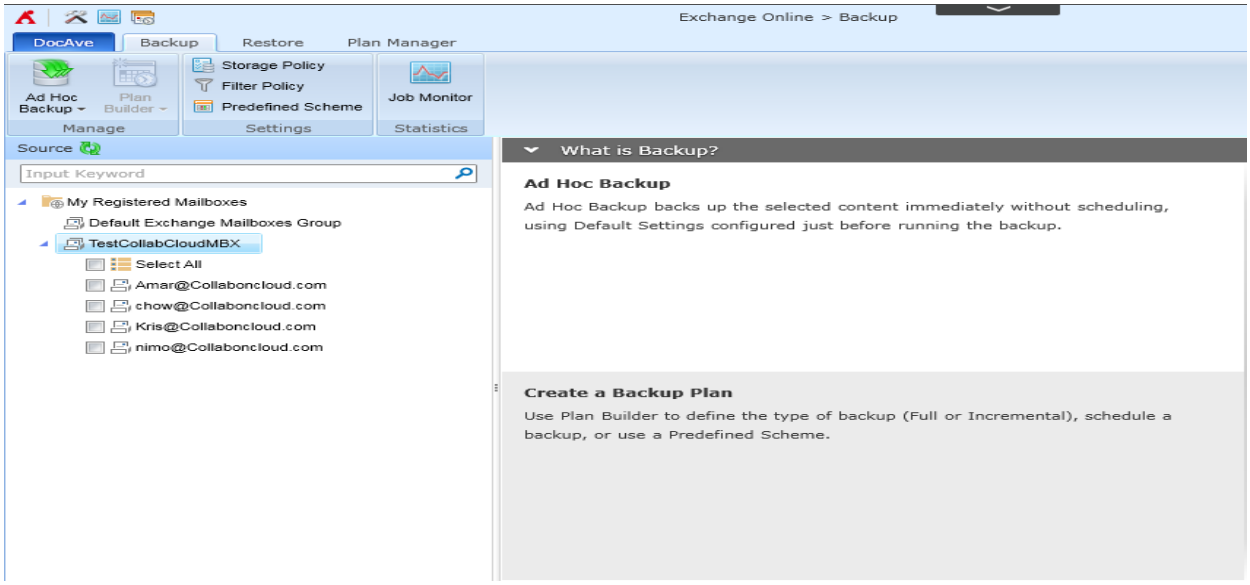
To launch Exchange Online Backup and Restore and access its functionality, complete the following steps:

1. Log in to AvePoint Online Services and navigate to DocAve Online.

 © 2016 NetApp, Inc. All rights reserved.

The DocAve tab displays all modules on the left side of the window.

2. From the DocAve tab, click Data Protection to view the backup modules.
3. Click Exchange Online Backup & Restore to launch the module.



To back up Exchange Online content, complete the following steps:

1. Click the My Registered Mailboxes node containing the relevant registered mailboxes.
2. Select an Exchange Mailboxes group on the tree to build a plan to back up all of the mailboxes included in this group and the mailboxes added to this group in the future. You can select objects throughout the mailboxes, but you cannot select the mailbox group and the mailboxes in the other groups at the same time.
3. Choose to perform either a backup using Ad Hoc Backup or the Plan Builder.

   Note: Frequent consecutive full backups have a tendency to repeatedly back up the same data, which fills disk space quickly. For best results when conducting high-frequency backups, NetApp recommends using incremental backups. Incremental backups save time and storage space by backing up only the differences between incremental backups or an incremental backup and a full backup, instead of backing up the entire source location

The backed-up data can be restored to its original location or another location in Exchange Online or a storage location. To use in-place restore to restore granularly backed-up data to its original location in Exchange Mailbox, complete the following steps:

1. Log into AvePoint Online Services and navigate to DocAve Online.
2. From the DocAve tab, click Data Protection to view the backup modules.
3. Click Exchange Online Backup & Restore to launch this module. Select the appropriate restore type based on where the content is restored.
4. Specify the restore settings to define the conflict resolution behavior.

   Note: The restore options can be set to in-place restores or to out-of-place restores to different storage locations as `.pst` files.

5. Click Finish.

   Note: For detailed steps, see the DocAve Online 3 User Guide.

 © 2016 NetApp, Inc. All rights reserved.

4.1 Solution Advantages

NetApp enables administrators to have complete control over Office 365 data, whether it's "all in" or in a hybrid model. The solution offers the following advantages:

- Reduction in overall management complexity of Office 365 in a hybrid model
- Simplified user and permissions management
- Data protection and monitoring:
  - Backup and restore of entire SharePoint Online, OneDrive for Business, and Exchange Online instances
  - Backup of site collections, sites, lists, mailboxes, and more
  - Item-level recovery for all SharePoint Online, OneDrive for Business, and Exchange Online components
  - Export Exchange Online backup data as a personal storage table (`.pst`) file
  - Restore content directly to storage locations, including NetApp FAS system and NetApp AltaVault
- The same backup SLA in the cloud as on premises
- Granular content protection and failover capabilities
- On-demand content restructuring, user solutions, and site elements deployment
- Customization of reporting, synchronization, and publication of content across sites and mailboxes

5 Data Protection Strategy

The business model for every organization evolves on a daily basis; therefore, security for Office 365 data is essential (based on the customer's requirements). Having a second, secure copy of the data is always a best practice, especially for data that resides in the cloud. Customers baselines their existing on-premises implementation with Office 365 offerings and want the same level of protection, administration, and security with Office 365.

Microsoft is responsible for protecting data where it resides, from the application layer down. The customer is responsible for its data. Apart from the above, such backups can be used as an alternative to moving information out of Office 365 back to on-premises servers and can be used to access the content even if the Exchange Online and SharePoint Online environment goes down. For example, there is no special administrative setting to defend against an Office 365 service outage. The only remedy to avoid lack of access to the Office 365 environment and to retrieve old data is a backup copy of the Office 365 data.

Office 365 backup and retention policies protect customers from data loss, but in a limited way; they are not intended to be a complete backup solution. Customers leveraging Office 365 (primarily Exchange Online, SharePoint Online, and OneDrive for Business) want their data protected to enable recovery if disaster or operational issues occur.

Together, NetApp and AvePoint provide Office 365 customers with backup services for Exchange Online, SharePoint Online, and OneDrive for Business. This solution enables customers to daily execute full and incremental backups and perform search and restore operations whenever there is a risk of data loss due to an unexpected purge or other wide range of causes.

6 Best Practices

NetApp recommends the following best practices:

- Use storage location physically closer to the Office 365 tenant.
- Create multiple plans for backup depending on Office 365 site topology.

 © 2016 NetApp, Inc. All rights reserved.

- Create and use multiple service accounts.
- Turn-on encryption and compression on FAS and AltaVault.
- Stagger backup plan execution.
- Run up to nine concurrent executions per backup job because every concurrent execution is for one site collection.

For example, if backing up 2,000 site collections, you would complete the following steps:

1. Split the backup off site collection into five plans, each having 400 site collections.
2. Use filter policy to split the site collections to multiple plans or create multiple groups and split the sites within them.
3. Create five service accounts to execute each plan.
4. Stagger the plans to execute a full backup operation at different times of the day.
5. Use the same plans to perform incremental backups.

7 Summary

Based on NetApp storage and DocAve Online, Office 365 customers can now do much more than just perform granular backups and restore operations of their Exchange Online, SharePoint Online, and OneDrive for Business data. NetApp offers compelling solutions for Office 365 to meet customers' business requirements. Regardless of the deployment model you choose, NetApp has the solution portfolio and the expertise to help you navigate the model's lifecycle, from planning and design to implementation, deployment, and management. Given the pace of change in both on-premises and cloud-based messaging and collaboration capabilities, a thorough analysis of all the options is essential to help you to deliver the right solution for your organization.

In today's tight fiscal environment, many enterprise customers are evaluating the entire package cost, not just the up-front purchase price. NetApp's strength is in reducing complexity and increasing efficiency and availability while providing the best solution to lower recovery point and recovery time objectives.

References

The following documents were referenced in this report:

- TR-4481: Hybrid Deployment for Messaging and Collaboration on NetApp Storage
  https://fieldportal.netapp.com/content/290038
- NetApp AltaVault Cloud-Integrated Storage
  http://www.netapp.com/in/products/protection-software/altavault/
- DocAve Online Technical Overview
  http://www.avepoint.com/assets/pdf/technical_overview/DocAve_Online_Technical_Overview.pdf
- DocAve Online 3 User Guide
  http://www.avepoint.com/assets/pdf/sharepoint_user_guides/DocAve_Online_User_Guide.pdf

Appendix

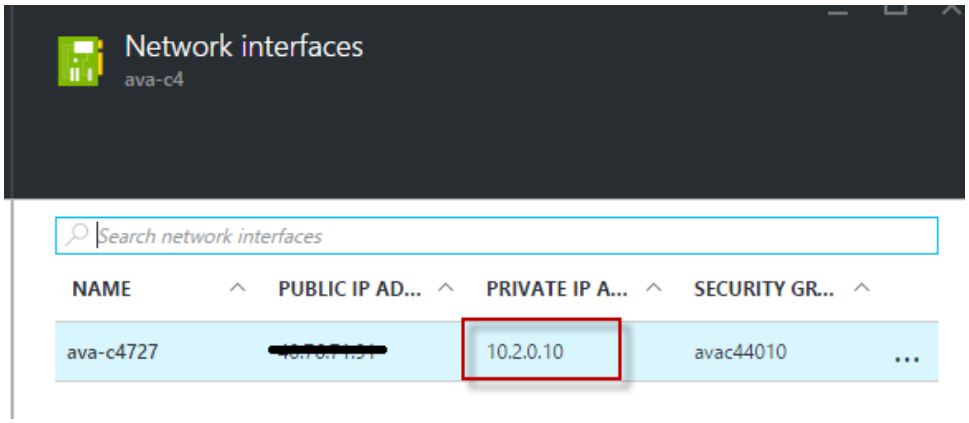
Set Up AltaVault Azure VM with SFTP Server for DocAve Online

To set up AltaVault Azure VM with SFTP Server for DocAve Online, complete the following steps:

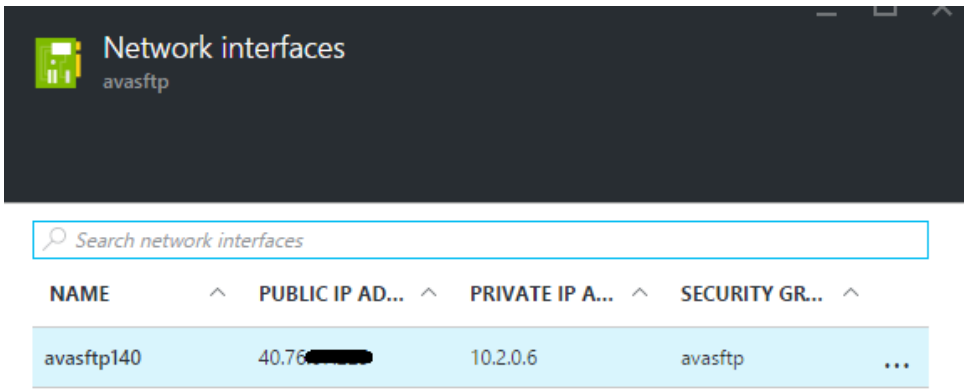
1. Set up an AltaVault cloud integration storage using the steps in the section titled "Deploying a Microsoft Azure Virtual Machine" in the "NetApp AltaVault Integrated Storage 4.1 Installation and Service Guide for Cloud Appliances."

 © 2016 NetApp, Inc. All rights reserved.

2. After the AltaVault VM is created, the VM should have a public IP address and an internal IP address in the Azure private virtual network (VPN). Save the private IP address for later to set up the CIFS and SFTP servers.

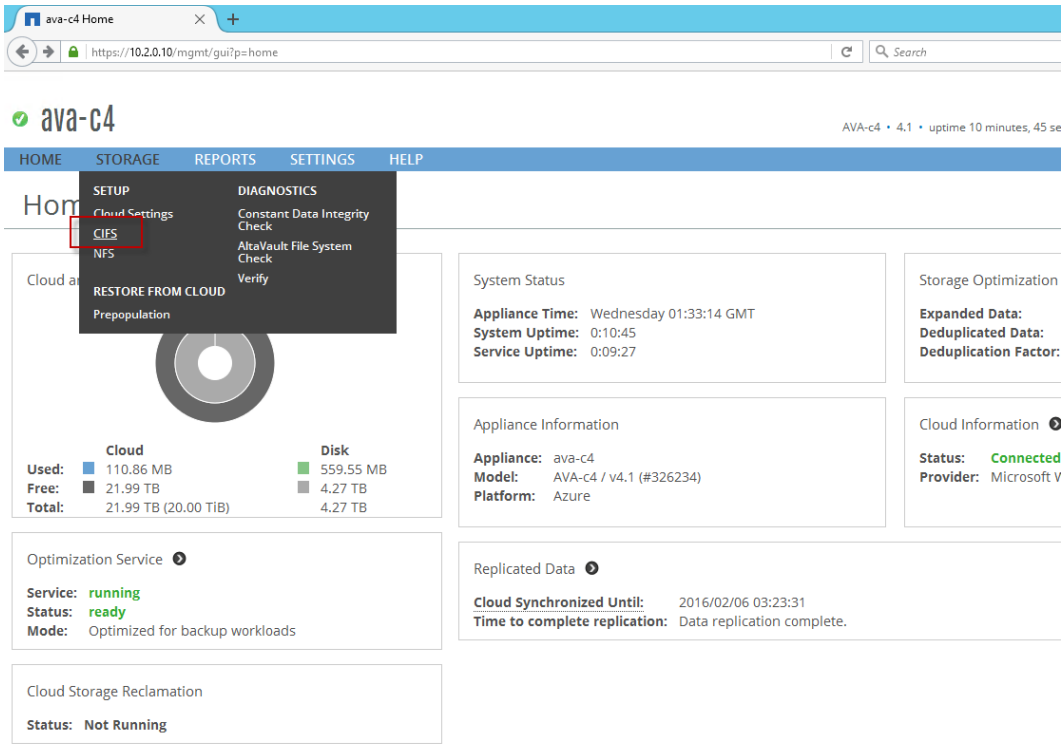


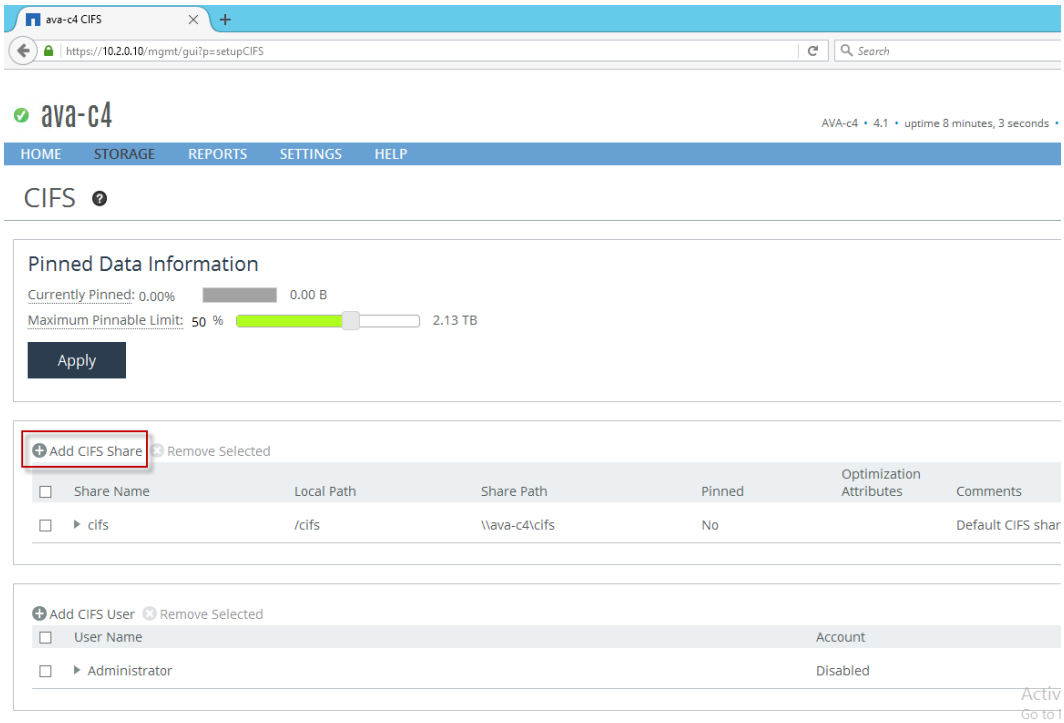
3. Provision another Windows VM (or Linux VM) that runs SFTP server. The VM is in the same Azure VNET that provisioned the AltaVault VM. In this example, a Windows VM is provisioned in the Azure VNET and subnet. Record the public IP address to configure the NetApp AltaVault device at DocAve Online service at a later time.



4. Enable and log in to the AltaVault web management UI.
5. Click CIFS to create a default CIFS share that the SFTP server uses for data storage.

 © 2016 NetApp, Inc. All rights reserved.



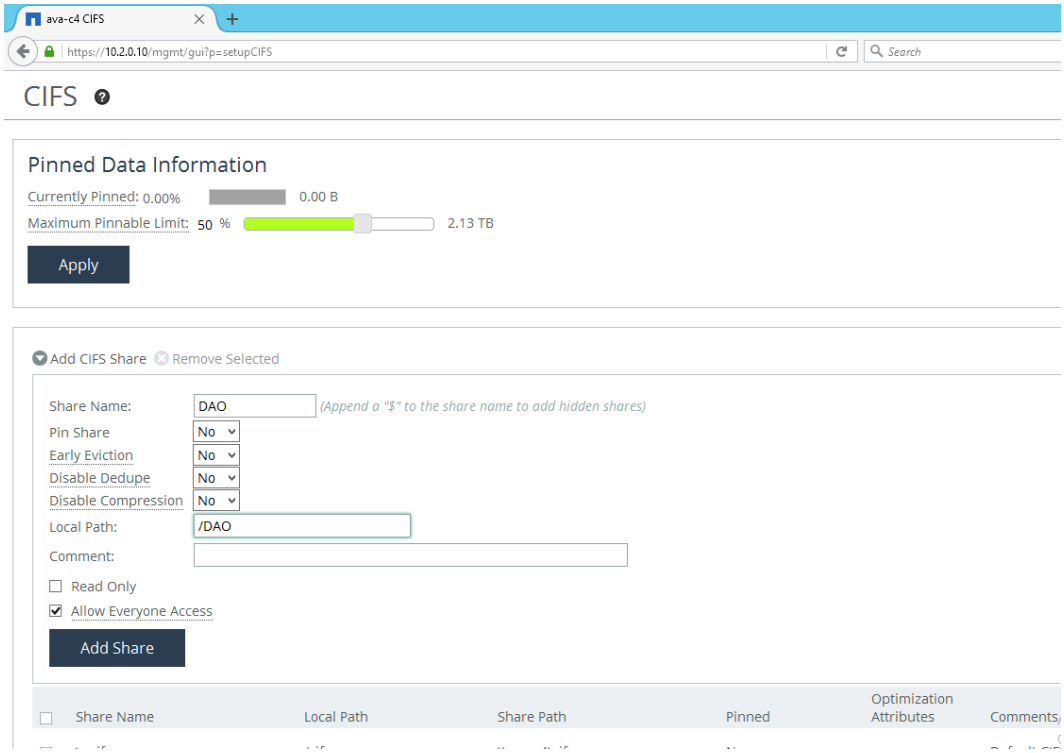


Set Up SFTP Server on Windows Server

To set up an SFTP server on a Windows server, complete the following steps:

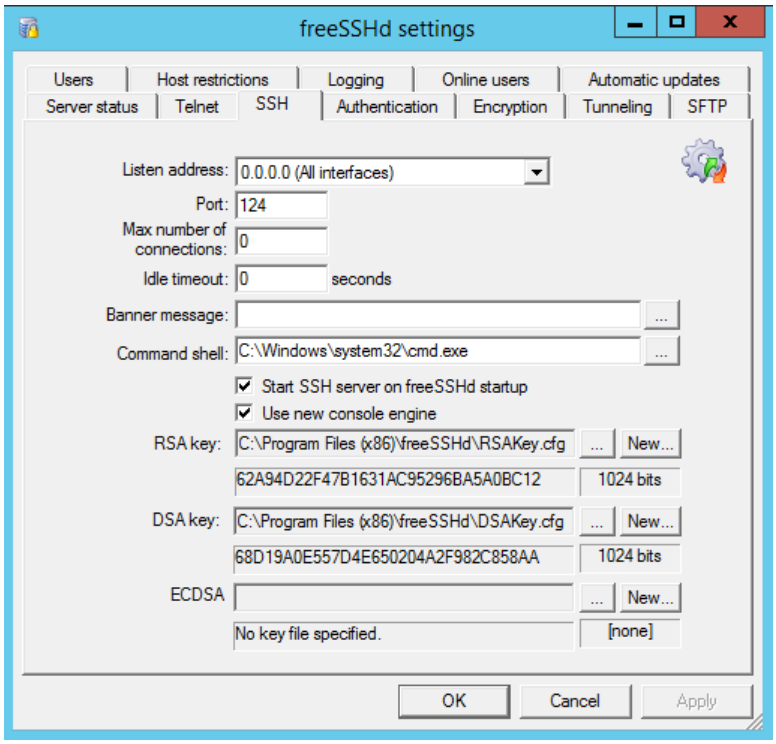
 © 2016 NetApp, Inc. All rights reserved.

1. Because the SFTP server VM is restricted, the AltaVault VMs are in the same Azure private VNET, and the CIFS share access is only inside the same protected subnet, select the Allow Everyone Access option when configuring the CIFS share.



2. If adding a CIFS share requires a user name and password, configure the user that is allowed to access the CIFS share.
3. Remotely log in to the SFTP server VM. In this example, the FreeSSHD SFTP server is configured to use port 124.

 © 2016 NetApp, Inc. All rights reserved.

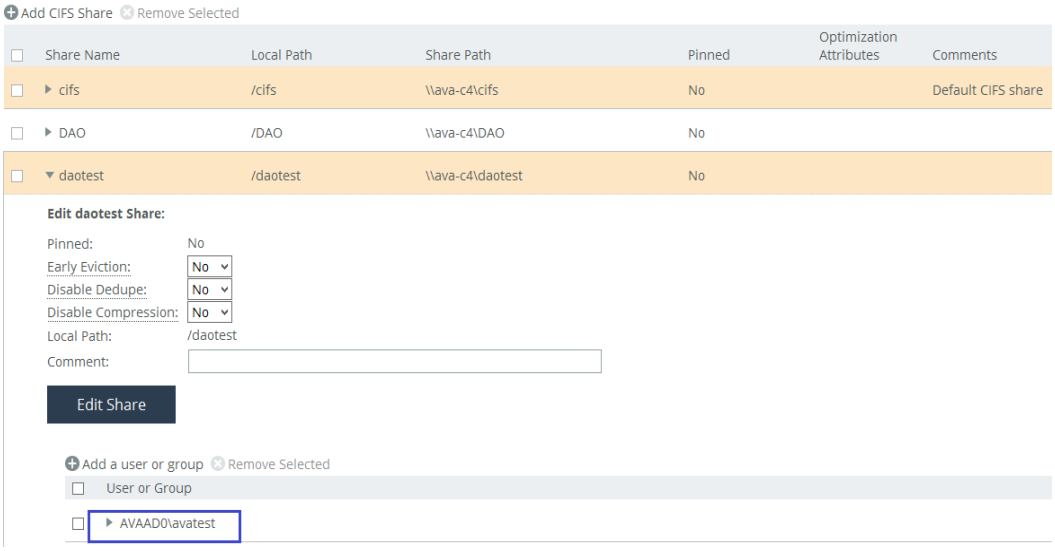


Note: To preserver the FreeSSHD configurations after the SFTP server reboot, configure FreeSSHD to run as a Windows service.

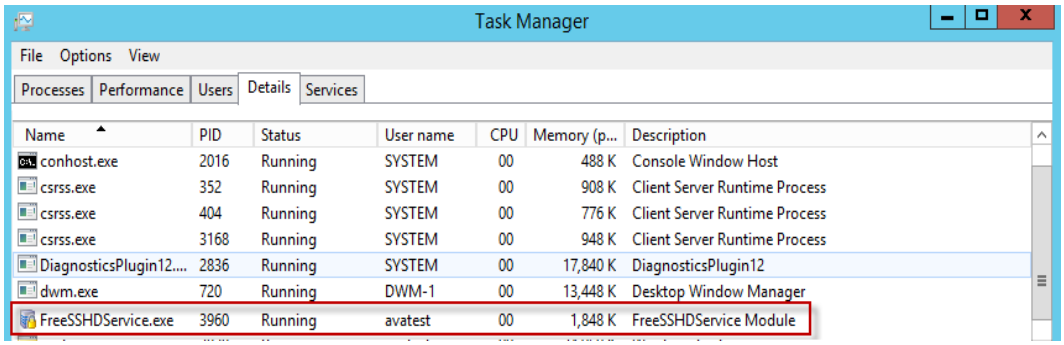
Note: If you are not using AD DC, then configure the CIFS share as Allow Everyone Access and set the SFTP home path to a UNC path as `<AltaVault_VM_private_IP>\<CIFS_share>`.

Note: If the AltaVault CIFS share is configured so that it is only accessible by certain Windows AD accounts, then an AD DC must be available and both AltaVault VMs and the SFTP server VMs must be configured to use the AD domain. The FreeSSHD service account logon must use the same AD user to run the service instead of running with the system account.

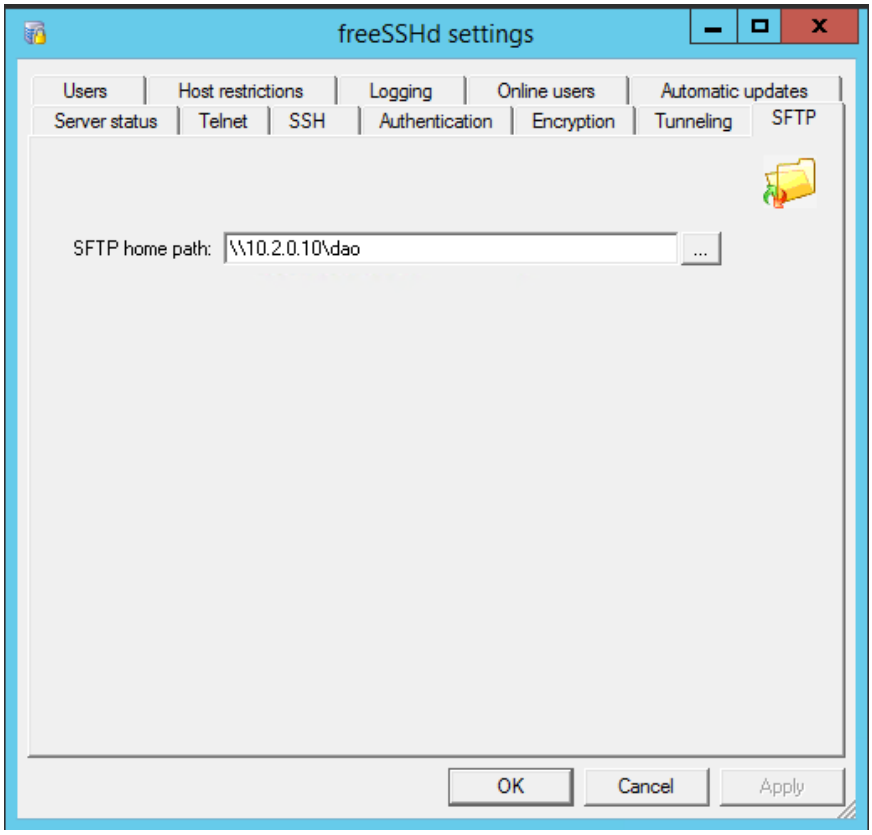
Note: In this example, when using the AD account to access AltaVault CIFS share, the AD account `AVAAD0\avatest` is used to access the AltaVault CIFS share and run FreeSSHD SFTP server.



 © 2016 NetApp, Inc. All rights reserved.

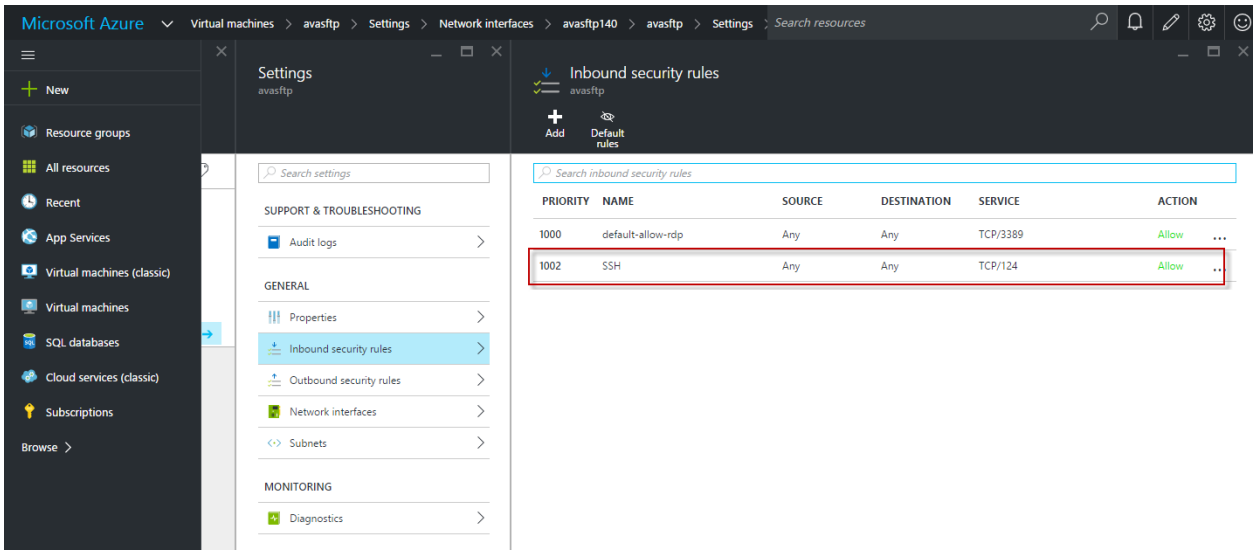


4. In this example, the AltaVault VM private IP address is `10.2.0.10` (identified in step 2) and the CIFS share is `dao` (added in step 5); therefore, the SFTP home path is set to `\\10.2.0.10\dao`.



5. Configure the SFTP server VM network security group (NSG) to enable SFTP access from the public IP address. As a result, the DocAve Online agent can access the SFTP server.

 © 2016 NetApp, Inc. All rights reserved.



Version History

Version	Date	Document Version History
Version 1.0	May 2016	Initial release.

 © 2016 NetApp, Inc. All rights reserved.

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

Copyright Information

Copyright © 1994–2016 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, Go Further, Faster, AltaVault, ASUP, AutoSupport, Campaign Express, Cloud ONTAP, Clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, GetSuccessful, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NetApp Fitness, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, RAID-TEC, SANshare, SANtricity, SecureShare, Simplicity, Simulate ONTAP, SnapCenter, SnapCopy, Snap Creator, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, SolidFire, StorageGRID, Tech OnTap, Unbound Cloud, WAFL, and other names are trademarks or registered trademarks of NetApp Inc., in the United States and/or other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. A current list of NetApp trademarks is available on the web at http://www.netapp.com/us/legal/netapptmlist.aspx. TR-4508-0516