Dell EMC Fluid File System Security Best Practices

FluidFS Systems Engineering
Dell EMC
March 2017
The information in this publication is provided “as is.” Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Copyright © 2017 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners.

Dell believes the information in this document is accurate as of its publication date. The information is subject to change without notice.
Table of Contents

1. Preface ................................................................................................................................. 1
2. Introduction .......................................................................................................................... 2
  2.1. FluidFS Overview ........................................................................................................... 2
3. Deployment Considerations for a Secure FluidFS Installation ........................................... 3
  3.1. Physical Access Security ................................................................................................. 3
    3.1.1 Power Button .............................................................................................................. 3
    3.1.2 VGA Console ............................................................................................................. 3
    3.1.3 USB Ports ................................................................................................................ 3
    3.1.4 LOM Port ................................................................................................................ 4
    3.1.5 Controller Removal ................................................................................................. 4
  3.2. Cabling Considerations - Network and SAN Fabrics .................................................... 4
4. Securing the Management Path ............................................................................................ 5
  4.1. Secured Management ...................................................................................................... 5
    4.1.1 Secured Management via VLANs .............................................................................. 5
    4.1.2 Secured Management via Dedicated Management Ports ......................................... 5
  4.2. Diagnostic FTP Access .................................................................................................... 5
  4.3. Support Access ............................................................................................................... 6
  4.4. Remote KVM Access ...................................................................................................... 6
  4.5. UI Session Expiry .......................................................................................................... 6
  4.6. Login Banners ................................................................................................................ 6
    4.6.1 DSM Login Banner .................................................................................................. 6
    4.6.2 FluidFS CLI Login Banner ...................................................................................... 7
  4.7. Turning off VAAI ............................................................................................................ 8
  4.8. Domain Users as FluidFS Administrators ...................................................................... 8
  4.9. Multitenancy and Administrative Scope ........................................................................ 8
    4.9.1 Restricting Global Admins from modifying Tenant Objects .................................... 8
    4.9.2 Restricting Tenant Admins from managing volumes .............................................. 9
  4.10. DSM Users vs. FluidFS Administrators ...................................................................... 9
5. Securing the data path ............................................................................................................ 10
  5.1. Limiting access to Shares by Subnet .............................................................................. 10
    5.1.1 Up to FluidFS v5 ...................................................................................................... 10
    5.1.2 FluidFS v6 onwards ............................................................................................... 10
  5.2. Local User Accounts ...................................................................................................... 11
    5.2.1 Password Expiry ...................................................................................................... 11
    5.2.2 Password Complexity Check .................................................................................. 11
  5.3. SMB Protocol Security ................................................................................................... 12
    5.3.1 Message Signing Per Tenant ................................................................................... 12
Acknowledgements

This white paper was produced by the FluidFS System Engineering and reviewed by the broader FluidFS Engineering team.

| Authors: | Ishraq Ahmed, and the FluidFS System Engineering team. |

Feedback

Please give us feedback on the quality and usefulness of this document by sending an email to:
FluidFS-System-Engineering@Dell.com

Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Mar 21st, 2014</td>
<td>First release</td>
</tr>
<tr>
<td>B</td>
<td>Mar 24th, 2014</td>
<td>Updated section on Security Vulnerability scans</td>
</tr>
<tr>
<td>C</td>
<td>Feb 17th, 2015</td>
<td>Updated for the FluidFS v4 release.</td>
</tr>
<tr>
<td>D</td>
<td>Sep 13th, 2015</td>
<td>Updated for the v4.0.210020 release. (added VAAI information)</td>
</tr>
<tr>
<td>E</td>
<td>Jan 2nd, 2016</td>
<td>Updated for the FluidFS v5 release.</td>
</tr>
<tr>
<td>F</td>
<td>Mar 7th, 2017</td>
<td>Updated for the FluidFS v6 release.</td>
</tr>
</tbody>
</table>
1. Preface

Dell network-attached storage (NAS) systems based on the Fluid File System (FluidFS) deliver scalable and highly available enterprise-class file services to clients running Microsoft® Windows®, Linux, and UNIX operating systems via the Server Message Block (SMB) protocol and Network File System (NFS) protocols. FluidFS supports protocol versions up to SMB 3.1.1 and NFS v4.1.

Dell Compellent® FS8600 clusters running FluidFS v6 can be managed via a Command Line Interface (CLI) or using a graphical user interface, Dell Storage Manager® (previously known as Dell Compellent® Enterprise Manager, and interchangeably referred to as DSM or EM in this document).

Dell encourages customers to consider security best practices while deploying new storage solutions. This paper describes security considerations for NAS storage systems and recommends best practices for assuring acceptable security when using FluidFS-based NAS solutions from Dell. It is intended for storage and security administrators who want to improve the overall security of their networked storage infrastructure.

As is typical with any other information technology infrastructure component, an increase in the overall level of security might result in a reduction in ease-of-use. One must be cautious when applying these configuration changes to Dell FluidFS NAS systems to avoid unexpected interruption of required services.

This paper is divided into four parts:

- Part I: Deployment considerations for a secure FluidFS installation
- Part II: Configuration for securing the management path
- Part III: Configuration for securing the data path
- Part IV: 3rd party tools for scanning for security vulnerabilities

The target audience for this paper is solution architects, system administrators, network administrators and IT managers. The reader is assumed to be generally knowledgeable about Microsoft Windows and Linux operating systems, SMB and NFS protocols, network technologies, file system permissions, and user authentication technologies.
2. Introduction

2.1. FluidFS Overview

FluidFS is an enterprise-class distributed file system that gives customers tools for easily and efficiently managing file data. FluidFS removes the scaling limitations of traditional file systems. It also supports scale-out performance and scale-up capacity expansion, all within a single namespace for easier administration. Because FluidFS optimizes both performance and scalability, it is an excellent choice for a wide range of use cases and deployment environments.

A Dell FluidFS appliance can be managed via a Command Line Interface (CLI) and/or a graphical user interface, and utilizes either an iSCSI SAN or a Fibre-Channel SAN to access the storage array.

FluidFS version 6 introduces multitenancy. Several CLI commands now have two different locations in the CLI hierarchy depending on whether or not multitenancy is in use.
3. Deployment Considerations for a Secure FluidFS Installation

Securing a FluidFS system starts with overall solution design and deployment planning. Before implementing a FluidFS NAS system, a complete and thorough assessment and review of physical access, network layout, security policies, administrative and role based access, protocol usage, partitioning of sensitive data, existing and new access requirements, must be completed and documented.

3.1. Physical Access Security

As with any IT infrastructure, physical access to the FluidFS system must be protected to avoid security breaches. There are several variants of FluidFS Appliances. The picture below uses the FS8600 1G as a sample to show the physical ports and their intended purposes. The descriptions with a dotted line around them have security considerations.

![Figure 2: Securing Physical Ports](image)

**3.1.1 Power Button**

The Power LED / Button combo switch is recessed to avoid accidental use, and the combo with the LED makes it non-obvious on the back of an appliance. Tapping this button cleanly shuts down a controller. Shutting down one controller takes the system to a degraded mode. Shutting down both controllers takes down the NAS Service.

**3.1.2 VGA Console**

The physical console allows some additional recovery accounts such as "resetmypassword" (for resetting a lost Administrator password) and "enableescalationaccess" (for advanced troubleshooting when the normal "support" account is unavailable) both of which have well-known passwords. Therefore, protecting access to the VGA console is important for security purposes.

**3.1.3 USB Ports**

While the most common purpose is to connect a keyboard, a USB port can also be used to connect an external USB drive to exchange data. Even though one can plug in a USB drive, any data can be transferred to/from the drive only through a support account shell or through an escalation account. There are some non-Dell locking solutions available to physically lock a USB port from being accessed.
3.1.4 LOM Port

The LAN-On-Motherboard (LOM) dual-purpose port on each controller is intended for the optional dedicated out-of-band management subnet, and also for remote KVM access via the embedded baseboard management controller (BMC). Even though it is a single physical port per controller, there are two PHYs behind it, one for use by FluidFS for secured management, and one by the BMC for Remote KVM (used for support). Remote KVM feature requires the use of the "support" account's password. Security of this port is important because one could access the VGA console remotely through it. The IP addresses for the LOM ports are configured using the CLI or DSM. The LOM ports may also be enabled/disabled via the CLI or DSM.

```
CLI> environment network management BMC-network edit 0 192.168.10.101
255.255.255.0 192.168.10.1
CLI> environment network management BMC-network edit 0 192.168.10.101
255.255.255.0 192.168.10.1
CLI> maintenance support security support-access bmc-enable
CLI> system internal security support-access change-password
```

3.1.5 Controller Removal

Each of the two controllers shown in the picture above can be removed from the appliance by depressing the orange latch locks and pulling on the handles. Removing the controller immediately powers it down without allowing the cache to flush. The best way to protect from accidental or malicious removal of a controller is to use whole-rack locking solutions available from several vendors including Dell.

3.2 Cabling Considerations - Network and SAN Fabrics

The use of VLANs (either tagged or untagged) offers additional Layer-2 security by providing traffic separation. Make sure to adhere to the network requirements set forth in the FluidFS Deployment Guides. It is important to note that FluidFS requires all Client Network ports to be in the same broadcast domain. FluidFS doesn't allow partitioning of physical ports in such a way that some Client network ports belong to one VLAN and others belong to another.

For the Fibre Channel version of FS8600, the InterConnect network ports are recommended to be left on a separate switch-based VLAN of their own. InterConnect network carries FluidFS internal cluster communication traffic only, and it mostly IPv6 based.
4. Securing the Management Path

There are several configuration settings in FluidFS and Dell Storage Manager to tighten up the security of the management path.

4.1. Secured Management

FluidFS supports two levels of Secured Management (Out-of-band Management). One at the physical layer by only allowing management over a dedicated physical path, and another at the VLAN layer by designating one Client Subnet as a Secured Management Subnet and preventing management traffic over any other VLAN/subnet.

4.1.1 Secured Management via VLANs

Although individual subnets/VLANs are not traditionally considered a security primitive, FluidFS does allow designating one subnet as the management subnet. By doing so, the management protocols (HTTP, HTTPS, SSH, FTP, SOAP) are all restricted to using that one particular subnet/VLAN only.

The Secured Management feature can address several of the security vulnerabilities listed by 3rd party vulnerability scanners like Rapid7 and Retina.

Here is an example of a CLI command for configuring a management subnet/VLAN in FluidFS:

CLI> environment network management access subnet edit -PrefixLength 23 -VLANTag 240 -PrivateIPs 10.10.78.124,10.10.78.125 -PublicIP 10.10.78.126 -State Unrestricted

After configuring the management subnet, logout of all existing sessions, (CLI/DSM) and login through the Cluster VIP on this management subnet (referred to as “PublicIP” in the CLI command above) and then enforce the management restriction as follows:

CLI> environment network management access subnet edit -State Restricted

You will have to delete the FluidFS Cluster from DSM and register it back in using the new VIP in the restricted subnet before enforcing the management access restriction.

4.1.2 Secured Management via Dedicated Management Ports

While creating a subnet, it is also possible to optionally apply that subnet to the “Admin” interfaces (the LOM ports mentioned earlier). By doing so, all the management traffic will be restricted to the LOM ports only. When the restriction is in place, data traffic (such as SMB/NFS) is disallowed on the LOM ports.

First create a management subnet on the Admin interfaces as follows:

CLI> environment network management access subnet edit -PrefixLength 23 -VLANTag 240 -Interface Admin -PrivateIPs 10.10.78.124,10.10.78.125 -PublicIP 10.10.78.126 -State Unrestricted

And then restrict the management access to this subnet as follows:

CLI> environment network management access subnet edit -State Restricted

4.2. Diagnostic FTP Access

Diagnostic FTP access (via port 44421) in FluidFS is intended for uploading a Service Pack file for upgrade, for downloading diagnostic files for troubleshooting, or for downloading SNMP MIBs and the VAAI Plugin. It is not possible to access any actual data in the NAS volumes via the Diagnostic FTP. However, a diagnostic package is a simple gzipped tarball and it would be possible to mine information from it that can be utilized for other types of attacks.

Also, the “supportShell” directory in the FTP area contains a file for each “engineering” support session containing a transcript of that session. Therefore, the recommendation is to keep Diagnostic FTP access
4.3. **Support Access**

Support access allows a Dell Support person to login to the system without requiring the use of any Administrator passwords. Once logged into via the "support" account, the support user can access the CLI and a support shell for troubleshooting.

It is recommended to keep the support account turned off unless it is needed for troubleshooting.

```
CLI> maintenance support security support-access disable
```

4.4. **Remote KVM Access**

As mentioned in a previous section, Remote KVM access over the LOM ports utilizes the support account’s password.

- When shipped from the factory, the Remote KVM has a well-known password that is known to Dell Support.
- It is important to have a strong password for the support account even though the support account is disabled.

4.5. **UI Session Expiry**

The default timeout for a CLI session is 30 minutes (1800 seconds). This can be reduced by using the following command. The lowest allowed is 10 minutes (600 seconds).

```
CLI> maintenance support security ui-configuration edit
    -SessionExpirationPeriod 600
```

4.6. **Login Banners**

The use of login banners is a simple way to warn any possible intruders that may want to access your system that certain types of activity are illegal. At the same time, a login banner can also advise the authorized and legitimate users of their obligations relating to acceptable use of the FluidFS NAS system.

Login Banners are typically used to point out:

- what is considered proper use of the system;
- that the system is being monitored to detect improper or malicious use;
- that there is no expectation of privacy while using this system;
- and that there may be undesirable consequences to using the system in an improper way.

Both the FluidFS CLI and the DSM client allow the use of a login banner.

4.6.1 **DSM Login Banner**

DSM Data Collector can be configured to force any DSM Client to display a custom banner on the login screen. Logon to the DSM Data Collector Manager and go to the Security tab. You’ll see a Login Message field.
After making this change, any DSM client connecting to this DSM Data Collector will be forced to restart and display the login banner as follows:

### 4.6.2 FluidFS CLI Login Banner

A customizable login banner for the CLI is a most basic deterrent and can be configured using the
command:

```
CLI> maintenance support security ui-configuration edit -LoginBanner
"Access to this system is being monitored. Privilege comes with responsibility"
```

When logging into the FluidFS CLI, the banner is displayed before an administrator logs in.

### 4.7. Turning off VAAI

Dell provides the vSphere APIs for Array Integration (VAAI) plugin for FluidFS, which communicates with FluidFS via a SOAP based web API on the Client Network. This requires Apache to be running inside the FluidFS controllers which in turn could trigger some vulnerability scanners.

If VAAI is not required, we recommend disabling this feature using the following CLI command.

```
CLI> environment vmware settings disable-vai
```

### 4.8. Domain Users as FluidFS Administrators

FluidFS allows any standard Active Directory user to be made an administrator of the FluidFS system. This allows for a standardized mechanism to control which users have access to the administrative interfaces. One may also register a FluidFS Cluster with Dell Storage Manager using an AD user that has been made an administrator of the FluidFS cluster.

An AD user can be made an administrator using the command:

```
CLI> maintenance administrators add FS8600Prod IA.LOCAL demoUser1
```

When logging into the administrative interfaces, use the same format of the username as specified when adding the external user as administrator. (i.e., for example, don’t shorten the name to IA\demoUser1)

When multitenancy is enabled, note that only those users that are in AD forests joined by the default tenant can be administrators. Local users defined in any tenant can be made administrators as well.

### 4.9. Multitenancy and Administrative Scope

FluidFS has three levels of Administrators – **Global** Administrator, **Tenant** Administrator and **Volume** Administrator.

A Global Administrator has full control over all of the management of the entire Cluster including all its tenants. The Global Administrator is also referred to as System Administrator in some areas of the UI.

A Tenant Administrator can modify any aspect of the tenant and the NAS volumes that have been assigned to that particular tenant. The Tenant Admin also has view-only access to the default tenant. The tenant admin cannot view other tenants that are not assigned to that tenant admin.

A Volume Administrator is assigned one or more volumes to manage and cannot modify anything else in the cluster beyond those volumes. The Volume Admin cannot even see the other volumes in the same tenant, but has full view-only access to the rest of that tenant, and the default tenant.

The CLI command below adds an Active Directory standard user as an administrator and also grants Global Administrator rights to this person.

```
CLI> maintenance administrators add FS8600Prod IA.LOCAL demoUser1 -IsGlobal Yes
```

### 4.9.1 Restricting Global Admins from modifying Tenant Objects

When configuring a tenant, you can lock out the Global Admin from modifying any objects (such as NAS Volumes) that belong to the tenant by unchecking this checkbox in the Edit tenant Settings dialog:
4.9.2 **Restricting Tenant Admins from managing volumes**
For added management security, a Global administrator can configure a volume in any tenant to not be modifiable by the Tenant Administrator. This is not a foolproof method because this setting can be easily reversed by the Tenant Administrator. However, an event fires when this change is done.

4.10. **DSM Users vs. FluidFS Administrators**
When a FluidFS Cluster is registered with DSM, a specific FluidFS Administrator’s credentials must be provided. Multiple DSM users cannot share the same FluidFS Administrator’s credentials.

Since DSM also supports Active Directory based users, the ideal approach is to use the same exact user from AD to login to the DSM client and also register FluidFS with DSM. To accomplish this, the AD user must be added to FluidFS as an Administrator with Cluster Administrator scope as described in an earlier section.
5. Securing the data path

5.1. Limiting access to Shares by Subnet

5.1.1 Up to FluidFS v5

FluidFS provides the ability for an administrator to configure each individual volume so that all shares and exports *based on that volume* can only be seen and accessed from a specific Client Network subnet. This is a significant security feature that allows the administrator to control which VLANs expose which shares.

Note that this a NAS-volume-based feature and not a per-share or per-export feature.

There are two parts to configuring this feature:

1. Select (or create) a Client Network subnet that will allow access to this volume. This will be one of the Client Network subnets already configured on FluidFS.
2. Apply a “subnet restriction” to the volume and include the selected subnet in “allowed subnets”

The Security tab of the “Edit NAS Volume Settings” dialog allows an administrator to configure this feature. After enabling the subnet restriction by click the “Enabled” checkbox, and then select a subnet by clicking “Add”. (FluidFS v5)

This can also be accomplished via the CLI using the following commands: (FluidFS v5)

```
CLI> NAS-volumes edit subnet-restriction add-allowed-subnet engvol1 <NetworkID>
CLI> NAS-volumes edit subnet-restriction limit-to-subnets engvol1 Yes
```

Where `<NetworkID>` is one of the IDs displayed by the “CLI> networking subnets list” command.

5.1.2 FluidFS v6 onwards

With the introduction of multitenancy, FluidFS v6 broadens the mechanism by which one can limit access to shares to specific subnets/VLANs.

Instead of restricting one volume at a time, multitenancy allows you to create a tenant with multiple volumes and automatically restrict access to those volumes to specific subnets by configuring tenant VIPs on those subnets only. In addition to restricting data access, you also get the ability to apply management restrictions on this set of volumes by having a separate tenant administrator (as discussed in a previous section).
Here is an overview of the steps involved in setting up subnet restrictions in FluidFS v6 and beyond. Please see the FluidFS Administrators Guide for information on how to perform these steps.

1. Enable multitenancy if not already enabled.
2. Create a tenant.
3. Choose which subnets are allowed access, and define VIPs for the tenant in those subnets only.
4. If needed, join tenant to Active Directory or other external user database.
5. Move volumes to be restricted into this tenant.

Now any shares and exports created on these volumes are only accessible via the subnets that have VIPs defined for this tenant.

If you just upgraded from FluidFS v5 to v6, you’ll notice that the v5 mechanism has been obsoleted. The system will keep any pre-existing subnet restrictions, but will not allow you to create new ones.

### 5.2. Local User Accounts

#### 5.2.1 Password Expiry

SMB user accounts that are local to the FluidFS system can be secured by setting the passwords to expire, and choosing a suitable expiry time. (default is 6 calendar weeks)

If multitenancy is enabled, the following command sets the expiry to 30 days and enables password complexity checks:

```cli
CLI> multitenancy tenants tenant1 client-access authentication
local-users-settings edit -LocalAccountsPasswordNeverExpires No
-CheckPasswordComplexity Yes -LocalAccountsMaxPasswordAge 30D
```

If multitenancy is not enabled, then the command is:

```cli
CLI> client-access authentication local-users settings edit
-LocalAccountsPasswordNeverExpires No -CheckPasswordComplexity Yes
-LocalAccountsMaxPasswordAge 30D
```

This can also be configured in Dell Storage Manager via the File System tab -> Tenants -> <tenant name> -> Client Accessibility -> Local Users and Groups tab -> Local Users Security pane -> Edit Settings.

![Edit Local Users Security Settings](image)

Individual local users’ passwords can also be set to expire independent of the global setting using one of these commands (with and without multitenancy).

```cli
CLI> multitenancy tenants tenant1 client-access authentication local-users edit testuser1 -PasswordNeverExpires No
CLI> client-access authentication local-users edit testuser1 -PasswordNeverExpires No
```

#### 5.2.2 Password Complexity Check

Password complexity check is enabled by default. It can only be disabled via the CLI on a per-user basis as follows:

```cli
```
5.3. SMB Protocol Security

An administrator can configure a FluidFS cluster to only accept signed and/or encrypted communication from Windows/SMB clients.

5.3.1 Message Signing Per Tenant

SMB Signing is a feature through which communications using SMB can be digitally signed at the packet level. Digitally signing the packets enables the recipient of the packets to confirm their point of origin and their authenticity. This security mechanism in the SMB protocol helps avoid issues like tampering of packets and “man in the middle” attacks.

By enabling the “Force SMB Clients Signing” checkbox in the SMB Protocol Settings, an administrator can force all SMB clients connecting to FluidFS clusters to use message signing. This setting applies to all SMB Shares on the FluidFS tenant. A slight performance impact may be expected after enabling signing.

The following CLI command also accomplishes the same.

```
CLI> multitenancy tenants tenant1 client-access authentication protocols without-password-complexity-checks change-password testuser1
```

5.3.2 Cluster-wide Message Encryption

SMB Encryption provides end-to-end encryption of SMB data and protects data from eavesdropping on untrusted networks. SMB Encryption should be considered for any scenario in which sensitive or confidential data needs to be protected from packet snooping. Note that there is going to be a performance impact from any end-to-end encryption protection due to the additional CPU cycles needed for the encryption computations.

By enabling the “SMB Encryption Enforcement” checkbox in a tenants’ SMB Protocol Settings dialog, an
administrator can force all SMB clients connecting to the FluidFS clusters to use message encryption. This setting applies to all SMB Shares on the FluidFS tenant.

The following CLI command also accomplishes the same.

```
CLI> multitenancy tenants tenant1 client-access authentication protocols
SMB-settings edit -RequireMessageEncryption Yes
```

### 5.3.3 Encryption for Specific Shares

Instead of requiring all clients connecting to the cluster to sign or encrypt their messages, an administrator can configure AES-based encryption for specific shares that contain sensitive information.

![Edit SMB Share Settings](image)

The equivalent CLI command is:

```
CLI> multitenancy tenants tenant1 NAS-Volumes volumes tenant-voil SMB-shares edit tenant-share1 -RequireMessageEncryption Yes
```

Note that enabling AES-based encryption effectively prevents SMB1 clients from accessing FluidFS shares. Microsoft® considers SMB1 to be outdated and it should not be used in security conscious enterprises.

### 5.4. Users and Roles

Make sure that users have unique user IDs and that those IDs can be traced back to a specific user. Avoid generic multi-user accounts wherever possible. FluidFS provides events to notify the administrator of failed attempts to authenticate while accessing shares, and also if the security/ACLs on the file/directory being accessed do not allow a particular user to access them. Where possible, consider granting rights and privileges based on the user’s role in the enterprise.

For instance, in an IT department, instead of using the “Domain Admins” group for all employees, it is recommended to create other smaller groups that are role-based, and use those groups to provide minimal access suitable for the actual role the engineer plays in the IT department. As roles change, an employee can be moved from one security group to another thereby automatically limiting the rights afforded to the user.

If machine accounts are needed, make sure to have separate accounts for each machine/system. For instance, if there are several multi-function printer/copier/scanner devices uploading scans to a SMB share, configure each of those scanners to use a different user account instead of having them all use the same “generic” account.

When creating NAS volumes and partitioning data into Shares, it is highly recommended to organize data by security requirements. For example, don’t allow engineering department data and HR department data
to be on the same Share or even the same NAS Volume. This will allow the use of different access controls, data protection and compliance policies for each and makes security configuration simpler to manage.

5.5. **NFS and Security**

NFS clients and servers traditionally use AUTH_SYS or “UNIX Style” security. This allows the NFS clients to send authentication information by specifying the UID/GID of the UNIX user to an NFS Server such as FluidFS. Each incoming NFS request contains the UID/GID of the UNIX user. This method of identifying a user provides minimal security as the client can spoof the request by specifying the UID/GID of a different user. This method of identification is also vulnerable to tampering of the NFS request by some third party between the client and server on the network.

One can mitigate this by configuring the client to use a Directory Service such as NIS or LDAP where users and UID/GIDs are maintained by some central IT authority within the enterprise.

5.5.1 **Authentication Service vs. Directory Service**

While a directory service reduces the possibility of UID/GID spoofing, the highest level of security can be attained by the use of an external Authentication service such as a Kerberos Key Distribution Center (KDC) for validating the identity of both users and clients accessing the storage infrastructure. The Microsoft Active Directory Domain Controller is the only KDC that is currently supported by FluidFS. Note that in order to use kerberized-NFS, the Linux/UNIX clients must be configured to authenticate with AD as well.

The NFS server in FluidFS supports the three Kerberos authentication methods - krb5, krb5i, and krb5p. These are selected in the NFS Export settings.

```
CLI> multitenancy tenants tenant1 NAS-Volumes all-NFS-exports edit tenant-voll tenant_export1 -UnixStyle No -Krb5 No -Krb5i No -Krb5p Yes
```

Here is the DSM screen for editing NFS Export settings.

![Edit NFS Export Settings](image)
5.5.2 Requiring a Secure Port
The FluidFS NFS server defaults to requiring a source port number less than 1024 for incoming requests. The recommendation is to leave this enabled. This provides a minimal level of security from malicious user-space NFS clients trying to spoof UID/GIDs. However, there are NFS clients OS’es like AIX that require the use of higher port numbers, and will need the “Require Secure Port” checkbox unchecked.

5.5.3 Limiting NFS Client Access
While the default is to allow access from all Clients, security can be improved by configuring each NFS Export to be exported only to a specific client, client subnet, or clients within a Netgroup. This is done via the following set of CLI commands:

```bash
CLI> multitenancy tenants tenant1 NAS-Volumes volumes tenant-voll
NFS-exports add-acl
```  
Available commands:
- for-all-clients
- for-single-client
- for-clients-in-subnet
- for-clients-in-netgroup

Or via the following DSM screen while creating or modifying an NFS Export.

![Add Access Control for NFS Export](image)

Note that the Linux “showmount -e <Cluster VIP>” command will still list all the NFS Exports including those that are not allowed to be mounted from the client that’s running the “showmount” command.

5.5.3.1 Root Squash
In the NFS Export Access permissions, the “Trust Users” selection defaults to “All but root”. This setting is called “root squash”. It prevents a user with UID=0, GID=0 from being considered as root on FluidFS. If you want root to be included, use “Trust Users = Everybody”. FluidFS allows trusting “root” only on a specific client, a client subnet or a netgroup. For security reasons, FluidFS prevents you from configuring an NFS Export to trust “Everybody” on “All Clients”.

5.6. LDAP Configuration options

Although FluidFS supports the simplest Lightweight Directory Access Protocol (LDAP) configuration with just anonymous binding to an LDAP Server, it is highly recommended to use more secure methods that are also supported.

Slightly more security is offered by the use of a BindDN and BindPW where a particular user account in LDAP is used to authenticate with the LDAP server before performing any queries. We recommend the use of LDAP over Transport Layer Security (TLS) when credentials are sent over the wire, to avoid the risk of packet sniffers.

The highest security is achieved by the use of an LDAP server configured with an SSL Certificate that can be uploaded to FluidFS via DSM.

In DSM, click on File System tab -> Tenants -> tenant_name -> Client Accessibility -> Directory Services -> NFS User Repository (NIS or LDAP) -> Edit Settings
5.7. Joining an Active Directory Domain

As a side effect of joining a FluidFS NAS system to a Microsoft Active Directory Domain, the "Domain Admins" group gets added to the local Administrators group of the FluidFS system. This allows all Domain Admins to have full control over all data in the shares and exports of the FluidFS system.

Any AD group can be added or removed from the local Administrators group except for the "Domain Admins" group. Please escalate to Dell Support if you need to remove "Domain Admins" from the local Administrators group. They will point you to the following Support Shell command that can accomplish this:

    Node0:supportShell> lw-lsa-remove-domain-admins-from-administrators

5.8. Quota Settings

Quotas are traditionally not considered a security primitive, but it is the simplest line of defense to prevent against a malicious or errant script running with compromised user credentials from filling up a NAS volume and preventing other users of that NAS volume from writing to it. Note however, that the "root" account does not have any quota restrictions.

5.9. SMB Share Ownership

As soon as a new SMB share is created, grant ownership of that share to a small group in Active Directory. Ownership defaults to the Local Administrators group and Read/Execute access is provided to 'Everyone' by default. Access the share either as a Domain Admin or Local Administrator, and change its ownership to a different entity. Ownership must always be granted to a group instead of just one user for practical reasons more than security reasons.

When multitenancy is enabled, the ownership of a share in a tenant defaults to the Local Administrators group of that tenant.

5.10. ACLs and SLPs

That stands for Access Control Lists and Share Level Permissions. FluidFS defaults to an SLP of "Authenticated Users" on any new Share created. Visibility of the share can be further reduced by replacing it with some other much smaller Active Directory group.

When it comes to ACLs, the recommendation is to adhere to the principle of least access. A user must be given access only to those resources that are required by their job function, and nothing more. Additionally, always grant access permissions to a Group instead of a specific user. If the user changes groups as a result of a change in job function, access is automatically revoked.

NFSv4 ACLs are supported in FluidFS. Use nfs4_setfacl and nfs4_getfacl utilities from any Linux client to manipulate these ACLs.

The use of the MMC (Microsoft Management Console) Shared Folders snap-in is no longer required for granting Share Level Permissions (the use of MMC is still supported however). The Administrator can use the FluidFS CLI or the Dell Storage Client to grant SLPs as shown in the following screen:
to the share with a Windows client just to configure those ACLs). To do this, go to the Folder Security tab of the Edit SMB Share Settings screen.

5.11. **File Access Notifications – 3rd Party Auditing**

An important facet of a secured infrastructure is the ability to audit user activity on any file system.

FluidFS v5 introduced the File Access Notifications feature, which allows an external application to receive notifications when files are accessed or modified by a user. One such external application is Varonis Datavantage. It allows the administrator to monitor and report on file access activity on FluidFS NAS volumes.

5.12. **SACL based SMB file access auditing**

SACL auditing is a basic file auditing mechanism that only works with Windows/SMB clients. This feature allows administrators to keep a watch on sensitive files/folders and monitor which users have accessed or deleted them.

First enable the Auditing feature on a NAS volume by enabling one or both of the checkboxes shown below.
Then set one or more SACLs (System ACL) on a file or folder in the NAS volume that needs to be monitored. To set a SACL, right click on a file in Windows Explorer and select Properties -> Security Tab -> Advanced -> Auditing Tab. Then use “Add” and “Remove” buttons to set SACLs on the object.

Here is a sample screenshot of the Auditing tab from a Windows client:

Once a SACL has been set, any time that file/folder is accessed, FluidFS generates an auditing event which can be viewed in the File System Tab of Dell Storage Manager under Client Activity -> SACL Auditing Events.

SACL Audit events are also available in the FluidFS CLI as shown below:

<table>
<thead>
<tr>
<th>CLI&gt; events auditing list</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unique ID</td>
</tr>
<tr>
<td>21335698</td>
</tr>
</tbody>
</table>

The auditing logs can be exported from DSM by using the Save-Table-Data method that’s built into DSM. Click on anywhere in the Security Audit Events table and hit the Ctrl-S key combination to bring up a
dialog that lets you choose the export format.

They can also be exported via the FluidFS CLI using:

```
CLI> events auditing list --CSV -HeadlineSubText "FileName.txt"
```

This mechanism provides a fine-grained SMB protocol-specific monitoring capability, but doesn’t work if files are accessed over NFS.

The multitenancy feature in FluidFS v6 onwards is not supported by external auditing applications. Therefore, for security reasons, we recommend only one tenant be configured for external auditing. The built-in SACL based auditing doesn’t have this limitation.

### 5.13. SACL Auditing vs. File Access Notifications

As seen in the previous two sections, FluidFS provides two mechanisms to audit file system usage and activity. The following comparison can help you decide which one to implement to meet your security/auditing needs:

<table>
<thead>
<tr>
<th>SACL Auditing</th>
<th>File Access Notifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Built-into FluidFS and DSM.</td>
<td>Requires Quest Change Auditor for FluidFS</td>
</tr>
<tr>
<td>SMB Protocol Only</td>
<td>SMB in Change Auditor 6.8, NFS &amp; FTP (future releases of Change Auditor and FluidFS)</td>
</tr>
<tr>
<td>Allows capturing both Allow and Deny events. It is possible to identify who tried to access specific files/folders even if they were unable to.</td>
<td>No notification is sent if access to a file/folder is denied and therefore nothing was accessed. So, it is not possible to identify who attempted to access.</td>
</tr>
<tr>
<td>Basic search capability is provided, but no reporting or usage analysis.</td>
<td>Extensive search and powerful reporting built into Quest Change Auditor for FluidFS</td>
</tr>
<tr>
<td>Some overhead on FluidFS for tracking and managing the SACL auditing information.</td>
<td>Much lesser performance overhead on FluidFS because the tracking and reporting is offloaded.</td>
</tr>
<tr>
<td>Multitenancy compatible. Each tenant has its own SACL Auditing events.</td>
<td>Only one tenant may be configured for external notifications.</td>
</tr>
</tbody>
</table>

### 5.14. Access Based Enumeration

Turning on ABE for a SMB share is a very simple way to prevent users who don’t have access to a file or directory from being able to even see the file or directory when they browse the share. What’s hidden from view cannot easily be hacked. Note however, that the overhead associated with ABE does result in a small performance penalty especially when browsing large folders.

Enable ABE on any SMB share using:

```
CLI> multitenancy tenants tenant1 NAS-Volumes volumes tenant-vol1 SMB-shares edit tenant-share1 -AccessBasedEnumeration Yes
```

### 5.15. File Permissions Interoperability Policy

FluidFS has two ways it can store the Security information on any file or directory – Windows and UNIX.

Windows style provides the most fine-grained control over permissions and interoperates well with Microsoft Windows clients. The UNIX Interoperability Policy uses UNIX-style security permission bits (user/group/other, read/write/execute). If Windows policy is used, permissions can be managed from a Windows client only, and if UNIX policy is used, permissions can be managed from a UNIX/Linux client only. A newly created NAS volume defaults to using the Windows policy.

There is also a legacy MIXED style that is generally not recommended even for situations where the same
set of files needs to be accessed from a UNIX environment and a Windows environment. The right approach there is to use User-Mapping (either Manual or Automatic) to map users between a UNIX Directory (such as NIS or LDAP) and Active Directory.

Note that the Interoperability policy is set on a file/directory when it is created and changing the policy of a volume doesn’t change the policy on any files previously written to the volume. One would have to explicitly change the permissions on each file/directory to reset the interoperability policy of that file/directory. Because of this, changing the Interoperability policy on a volume after it has been in use for some time can lead to a lot of confusion and is strongly discouraged.

For Windows-only use-cases and for most cross-protocol use-cases, Dell recommends keeping the default Interoperability policy of Windows. For UNIX-only use-cases, choose the UNIX Interoperability policy.

5.16. Use of Firewalls
Most enterprises implement some sort of firewalling around their Data Centers to restrict unwanted network traffic. As is typical of any storage system, a FluidFS NAS system is definitely not designed to be left facing the Internet.

An exhaustive list of FluidFS TCP/UDP ports that are required to be left open for specific NAS services to be available, and for the proper functioning of a FluidFS NAS system, is provided in the Dell Fluid File System Support Matrix.

Firewalls may also be used to block specific vulnerabilities identified by 3rd party vulnerability scanners after consulting with Dell Support.

5.17. FTP Access
FluidFS v6 supports authenticated FTP/FTPS and also anonymous FTP.

Anonymous FTP is by definition a wide open and insecure access method. So if there is a business need to use anonymous FTP, please make sure that the FTP landing folder is chosen to not have any sub-directories with sensitive data that could be exposed.

Also, make sure that the landing folder for Anonymous access is distinct from the Regular landing folder for authenticated access.
5.18. Global Namespace

FluidFS v5 introduced the global namespace feature which allows multiple FluidFS clusters to be aggregated into a single namespace by the use of redirection folders. See the Administrators Guide for more details on how to implement a global namespace using FluidFS. The global namespace feature in itself doesn’t provide any additional security measures, beyond what each FluidFS cluster already provides. But there are some important aspects to remember:

5.18.1 Independent security domains

The security of each portion of the namespace is enforced by the FluidFS cluster that hosts that portion of the namespace. Even though the users see a “single” namespace, the security settings of the individual FluidFS clusters are independent of each other, and therefore care must be taken to ensure that any security settings applied to the root FluidFS cluster of the namespace are also implemented across all FluidFS clusters in the global namespace.

For example, while the shares of one FluidFS cluster in the namespace are configured to require SMB signing, shares on other clusters in the namespace may be easily overlooked leaving parts of the namespace vulnerable.

As a second example, the subnet restrictions applied on one FluidFS cluster will need to be separately applied on all the other clusters to keep the entire global namespace restricted to clients accessing via specific Client Network subnets/VLANs.

5.18.2 No ACL inheritance

Since the FluidFS clusters in a global namespace are really independent of each other, the files and folders hosted by other FluidFS clusters in the namespace do not inherit ACLs from the root of the namespace hierarchy.

Always make sure to have appropriate ACLs on all the file systems across all clusters in the namespace hierarchy to prevent unauthorized access to any portion of the namespace.

There are a variety of tools available for scanning for security vulnerabilities in a storage system. This section describes the testing performed by Dell and the findings. Most importantly, the methods of mitigating any findings are also listed.

Important note: Most vulnerability scanners don’t actually perform any real penetration testing. Instead they rely on revision strings of specific sub-components, reference known vulnerabilities of those sub-components, and list those vulnerabilities as potentially being present in the system being scanned. However, since Dell FluidFS is constantly evolving without necessarily modifying specific subcomponents’ revision strings due to external licensing restrictions, such approaches tend to result in false-positives.

6.1. FluidFS Configuration Used in Testing

The following configuration may be used in testing for security vulnerabilities using 3rd party vulnerability scanners:

- System Under Test (SUT):
  - A single Dell Compellent FS8600 10G iSCSI appliance running with:
    - FluidFS version 6 (Specifically 6.0.003169 or later)
    - Dell Storage Manager 2016 R3.1 running on Windows Server 2012
    - Another FS8600 system in a replication partnership

- Configuration of the SUT:
  1. Two client network subnets on the “Client” interfaces
     a. Two VIPs on each subnet
  2. A dedicated Management Subnet configured on the Admin interface
  3. System joined to Active Directory
     a. AD has a group called “My Department Users” containing Standard Users.
     b. AD has a group called “My Department Admins” containing two Domain Admin users.
  4. Local users’ passwords set to expire in 30 days
  5. LDAP Server configured with non-anonymous binding and using TLS with a certificate
  6. NFSv4 protocol enabled
  7. HTTP access disabled:
     a. VAAI interface disabled
  8. Require SMB signing
  9. Valid SSL certificate uploaded
 10. FTP service disabled
 11. Support password set, but Support Access disabled
 12. Anti-Virus (AV) Server configured (McAfee or other)
 13. NDMP backup DMA configured (Symantec NBU or Symantec BE or other)
 14. Replication partnership established with another FS8600
 15. NAS volume Vol1 configured as follows:
     a. Interoperability Style is Windows
     b. Hourly snapshot schedule with retention period of 24 hours
     c. Daily replication schedule to a NAS volume on the partner FS8600
     d. Quota settings enabled:
        i. Default User Quota set to 100GB
        ii. Default Group Quota for “My Department Users” set to 200GB
     e. One NFS export configured as follows:
        i. Access to “Everyone but root” from 3 specific clients on the client subnets
        ii. Access to “Everyone” from one specific client in the dedicated management subnet
Authentication methods:
- UNIX Style, Kerberos v5, Kerberos v5 Integrity – Disabled
- Kerberos v5 Privacy – Enabled
- Required Secure Port - Enabled

f. One CIFS share configured as follows:
   i. Share Level Permission for “All Authenticated Users” removed and replaced by “My Department Users” with Full Control.
   ii. Share ownership set to “My Department Admins”
   iii. AV scanning enabled
   iv. Access Based Enumeration enabled

6.2. Scan Reports and Mitigations
Dell continually performs security scans on FluidFS Maintenance Releases with a variety of 3rd party scanners using a system configuration similar to that described in the previous section, and can provide these reports upon request.

Please contact Dell Support to obtain this information along with suggested mitigations and responses to specific vulnerabilities.
7. Additional Resources

Referenced or recommended Dell publications and resources:

- FluidFS Technical Content
  http://en.community.dell.com/techcenter/storage/w/wiki/7425.fluidfs-technical-content
- FluidFS Support Matrix
  http://en.community.dell.com/techcenter/extras/m/white_papers/20441581
- http://kc.compellent.com/ Documentation and Best Practices for Dell Compellent FS8600 and Dell Compellent Storage Center
- http://dell.com/support Documentation for all other Dell products including PowerEdge, PowerConnect, and Force10
- http://DellTechCenter.com is an IT Community where you can connect with Dell customers and employees to share knowledge, best practices, and information about Dell products and your installations.