Integration Guide: Implementing FileNet P8 Content Manager with Network Appliance™ Storage Systems

Gangoor Sridhara, Network Appliance, Inc.

Bob Kreuch, FileNet, an IBM Company

TR-3535

Executive Summary or Abstract

Content and business processes have caused significant growth of unstructured data in an enterprise environment. Today's enterprises require a structured approach to manage the content and business processes effectively. The joint solution of FileNet P8 platform and Network Appliance storage systems provides enterprises the capability to archive and protect both business-critical content and business process data in an elegant way to manage a unified storage environment. This technical report discusses in detail the procedure to complete the installation of FileNet P8 platform system in a Network Appliance unified storage environment. This paper briefly discusses the procedures to install NetApp software tools such as SnapDrive®, Host Attach Kit (HAK), etc.

Table of Contents

1. Introduction

Corporate data belongs to three groups: structured, semi-structured, and unstructured data.

- Structured data - Data actively managed by a relational database application. A few examples of structured data are RDBMS Data, ERP Systems Data, etc.
- Semi-structured Data - Data loosely managed by an application. A few examples of semi-structured data include messaging/email environments.
- Unstructured Data - Data not controlled or monitored by any application or database server. Examples of unstructured data include user's home directory, incoming fax document, prints, and Microsoft® Office files.

Structured data tends to have very well defined processes or procedures for backup archival and compliance, semi-structured and unstructured data tend not to have such processes in a corporate environment. An enterprise must provide efficient methods for data access and the ability to scale the growth of content. Some examples of fixed content include electronic documents, faxes, images, and rich media files. Data generated from print, voice and electronic communication leaves Enterprise customers to solve their content management issues. Enterprise content management (ECM) enables people in an organization to manage such content. An ECM solution includes a wide range of solutions such as logical references to storage locations, searches and retrievals, and version control multilevel security. By deploying a joint solution from FileNet and NetApp, end users are able to design and configure a good ECM system. FileNet P8 platform includes back-end services, development tools, and applications to address enterprise content. FileNet P8 platform addresses business process management (BPM) requirements.

FileNet has a range of products to provide business solutions for document and content management needs. FileNet offers solutions for image services and content services requirements. FileNet P8 platform is a complete set of ECM solutions that supports both image and content services, including BPM capabilities.

Network Appliance (NetApp) storage systems provide unified storage solutions that serve data on both storage area network (block data) and network attached storage (file system) configurations. Software solutions enhance the data management solutions such as the ability to address backup, recovery, and efficient data replication features. Fast, high reliability and advanced data protection options are some of the key features of Data ONTAP® software.

By integrating FileNet Content Services product with NetApp storage system solution, users will be able to take advantage of joint solutions. Storage management, content backup, recovery, and scalability are some of the few features available with joint solutions. By deploying the joint solution of NetApp storage system and FileNet Content Services, users will be able to configure a robust ECM solution. FileNet P8 Platform supports fixed contents on a NetApp SnapLock® enabled storage setup to meet compliance requirements.

By taking advantage of the strengths of NetApp storage system solution with FileNet P8, enterprise customers will be able to address information lifecycle management (ILM) issues. This paper describes the steps required to deploy FileNet P8 platform and Network Appliance storage system solution. The combination of FileNet P8 platform and NetApp storage systems yield a highly available and scalable solution to solve any enterprise's most demanding enterprise content management and compliance challenges.

1.1 Background on Technical Issues

FileNet offers an advantage of storage pointers for document management paths with its enterprise content management solutions. This architecture eliminates the need for obtaining the physical storage path, improving the system performance. Tasks such as moving files and adding directories are handled centrally within FileNet Content Services. In addition to managing Email data, FileNet Content Service P8 product offers efficient ways to manage enterprise content.

In an ECM environment, enterprise customers expect a robust solution to address issues such as –

- Ability to search and retrieve on their network
    - FileNet Content Service P8 product supports this feature using titles and property names in plain language. This avoids complex file names. Regardless of the data or user location, simple file name is sufficient for search and retrieval.
- Ability to provide logical storage pointers instead of physical storage pointers
    - FileNet Content Service P8 is aware of the data and does not require physical storage pointers. This architecture improves performance yet shields the physical storage locations from users, adding a higher level of security.
- Ability to manage the version control when a document is opened for editing
    - P8 product supports this feature when a document is opened for writing by marking as checked out, while keeping the original copy protected.
- Ability for Open Architecture support
    - P8 system works with multiple (almost all) user interfaces. A common repository can support content belonging to various groups within the network. Should there be a need to develop custom applications in future; one may take advantage of P8 support.
- Ability to make the content “intelligent”
    - P8 system architecture uses Object-Oriented model to convert an ordinary file into intelligent content. Actions performed on an object (document) derive its properties such as user authentication.
- Ability for Load Balancing and Scalability
    - P8 system provides efficient queue management and load balancing features by using multithreaded approach. This design will address issues such as significantly higher load on a single server or unavailability and requests automatically rerouted to other servers.

NetApp storage system solutions offer compelling advantages to these content management scenarios. The ability to provision storage with primary and archived workload characteristics on a single system provides simplified management and leverages/minimizes IT skill sets, as users are required to only manage product and maintain a single system. In addition to significant growth of content data volume, a number of compliance regulations recently enacted globally mandates the archival of email and enterprise content and business process data. This requirement and the required ability to produce the data in a timely manner have driven enterprises to pursue a more structured and regulated archiving process.

1.2 Purpose and Scope

Purpose of this paper is to demonstrate the ease of product integration of FileNet P8 platform and NetApp storage systems. It is very important to note that this is not a substitute for the product documentation and release notes shipped with FileNet P8 platform and/or the target NetApp storage systems. It is very important to complete all the preinstallation tasks before attempting to install the software product. This paper will discuss steps required to prepare the Operating System (OS) and NetApp storage systems for FileNet P8 platform component installation and configuration.

This paper will discuss the requirement for installation of software products such as SnapDrive from NetApp and the procedure to configure the FileNet P8 platform in SQL Server environment on Windows® environment. FileNet P8 platform supports email management. However, this paper will not go into details of each FileNet P8 platform component or the NetApp software component installation and configuration details. In addition to FileNet P8 components, this paper will briefly discuss the installation of additional software products including the NetApp Host Attach Kit and SnapDrive software. This paper refers the readers to appropriate product installation and configuration supplied with your releases of software.

1.3 FileNet Content Services (P8)

Corporate data generated from various sources, such as paper documents, voice, and electronic communication, forms the enterprise content and is spread over an entire organization globally. Enterprise Content Management solution manages such data in an effective manner. FileNet Content Services is a leading enterprise content management solution as discussed in Section 1.1. FileNet Content Service P8 system has robust architecture to solve ECM issues.

FileNet P8 family of products provides a complete set of solutions to address enterprise content management. They include back-end services, development tools, and applications that address enterprise content and business process management (BPM) requirements. Client interfaces allow the access to Enterprise content data. Baseline components included in FileNet P8 family of products are content engine (CE), process engine (PE), application engine (AE), and rendition engine (RE) to address content management and BPM requirements.

Applications like Records Manager (RM), eForms, Capture, Email management, Team collaboration manager, and Web content manager sit on top of FileNet P8 platform. FileNet image manager (IS), content federation services, and image services resource adapter (ISRA) work below the FileNet P8 platform level. This architecture provides a robust solution to manage enterprise content efficiently.

Integrated solutions of FileNet P8 platform with NetApp storage systems offer a reliable, scalable, and highly available architecture to address enterprise content management by increasing operational efficiency. They also lower the total cost of ownership while increasing the total customer experience in the enterprise content management segment. In addition to this, FileNet P8 architecture enables business process automation and manages the content offering the compliance solution.

2. Infrastructure

This section of the paper, we will describe the necessary infrastructure for deployment of FileNet P8 platform environment. FileNet P8 platform is supported on Microsoft Windows environment. FileNet P8 can be configured to support compliance requirements as well as basic archiving requirements. To support compliant retention of data, content engine services rely on the storage system solution's ability to lock fixed content data in an immutable store. This paper briefly describes the procedure to configure NetApp Storage systems using Network Appliance SnapLock to achieve compliance data. For complete and detailed instructions on compliant data retention with Network Appliance SnapLock, refer to "Using SnapLock Compliance and SnapLock Enterprise with Data ONTAP 7G". Appendix sections list additional documentation in relevant to FileNet P8 and SnapLock setup environment.

Broadly there are four different configurations are available in FileNet P8 platform environment. The type of configuration helps to calculate the required number of servers. The possible four configurations listed below are-

- Baseline configuration – in which Content Engine server, Process Engine server, Rendition Engine and Image Services server are configured with Application Servers to form a FileNet P8 baseline configuration.

- Baseline configuration with optional components – In addition to baseline configurations, additional components are configured such as Capture workstation, eForms Designer, process simulation server, etc.
- Developer Configuration – helps to have a P8 platform system available for development team. In this configuration, various developer workstations are connected to content server and Image servers. In this configuration, content engine and process engines are shared among the development workstations.
- For demonstration purposes, all components of P8 platforms are to perform product demonstration, testing proof-of-concept and any development tasks on a single server. Currently Rendition Engine has to be installed on Windows 2000 server and not Windows 2003.

Deployment of FileNet P8 system requires Microsoft Windows 2003 or Windows 2000 server. In addition P8 platform requires Microsoft SQL 2000 server. Starting with content engine 3.5.2 release, FileNet supports SnapLock configuration to meet compliance requirements. Network Appliance recommends the deployment of application software and database server environments using either Fibre Channel SAN (FCP) or iSCSI protocols. Documentation and best practices for these application deployments are described in detail in several technical reports available in the Network Appliance Technical Library section.

P8 platform infrastructure requirements depend on the type of configuration deployed. Four possible FileNet P8 deployment configurations are discussed in this section. Baseline configuration includes a content engine server, process engine, and rendition engine server. Database server infrastructure is a requirement in FileNet P8 environment. Image Services and optional servers for implementing other components are also available to provide additional functionality and improved data management capabilities. Depending upon the workload, a database server can be configured on a dedicated server or on any of the servers within P8 system. , On Windows environment, a Windows Active Directory domain controller is required to complete the installation. P8 platform is a total ECM solution that includes optional Image Services configuration. For detailed procedure for the Image Services product integration details, refer to FileNet TR.

In our test setup, we used the baseline configuration. Following systems were used as part of FileNet P8 infrastructure. Number of NetApp storage systems integrated into the P8 platform environment depends on various factors such as amount of storage space required, backup, and high availability.

- Windows 2003 Service Pack 1 Enterprise Edition for Installing Exchange Server
- Windows 2003 Service Pack 1 Enterprise Edition for Installing SQL Server and CE Server
- Windows 2003 Service Pack 1 Enterprise Edition for Installing Process Engine Server
- Windows 2003 Service Pack 1 Enterprise Edition for Installing IS
- Windows 2000 Service Pack 4 Server for Installing Rendition Engine
- Windows 2003 Service Pack 1 Enterprise Edition for Application Server
- Appropriate Client workstations over the network
- NetApp FAS3050C storage system running Data ONTAP 7.1.1 for FileNet P8 storage requirement (Clustered system configuration is optional)
- NetApp FAS980 Storage System running Data ONTAP 7.1 for Storage Area Network Configuration
- NetApp R200 Storage System running Data ONTAP 7.1 for P8 storage archival

- NetApp SnapDrive software product version 4.1 for Storage management
- NetApp SAN Storage software product – Host Attach Kit 3.0
- Emulex LP9002L fabric attached adapter card and HBAnywhere software. For complete compatibility and support matrix, refer to The Compatibility and Configuration Guide for NetApp FCP and iSCSI Products.

Baseline configuration with optional components requires additional hardware infrastructure for installing eForms Designer, FAX Capture, Process simulator, and Process Analyzer server components. Optional components expand functionality of FileNet P8 platform configuration. Additional components such as FAX import and Capture workstations are necessary even in baseline configurations. Following figure displays the configuration to utilize the core FileNet P8 platform components in addition to optional components such as process analyzer and process simulator.

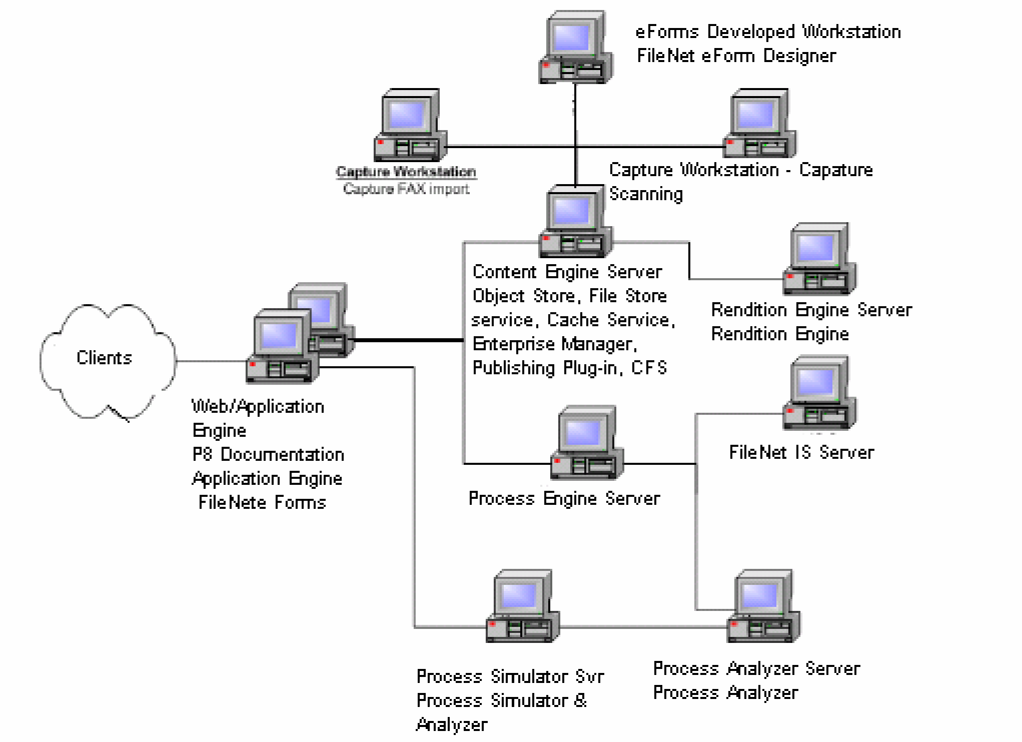


Figure 1: FileNet P8 Baseline Configuration with optional components

2.1 Infrastructure Related Tasks

It is necessary to prepare the system to be ready for installing FileNet P8 platform component software. Failing to complete the preinstallation tasks may prevent the software installation or show a different behavior.

This paper assumes that the NetApp storage systems are configured with the needed host attach kits. For this purpose, we used host bus adapter (HBA) card LP9002L from Emulex to connect from Windows servers to the NetApp storage system. For complete support matrix for this hardware, refer to NetApp support site. Note that configuration of storage area network is completely optional. This paper suggests installing the application software components and database server on locally configured drives. Content data on the networking environment works just fine.

In order to configure storage area network for installing SQL Server and FileNet P8 platform server components, one has to decide whether to use SAN or IP-based SAN storage configuration. This paper assumes a new installation of SQL Server and FileNet P8 platform components on NetApp SAN configuration using Fibre Channel protocol. Enable the necessary product licenses.

FileNet P8 platform supports SnapLock volume to meet compliance requirements to manage the fixed contents in addition to data in object stores. In our test setup, we used SnapLock for compliance volume configuration to store fixed content.

To install SAN host attach kit software; follow the FCP Installation Guide on http://now.netapp.com. Additionally, SAN Manager Software may also be installed. SAN Manager provides end-to-end Fibre Channel SAN management that enables NetApp customers to securely monitor and manage their enterprise storage infrastructure. To discover and monitor NetApp storage devices, SAN Manager requires a DataFabric® Manager server. If you require upgrading the HBA driver and firmware, refer to Host Bus Adapter documentation at NOW™ site.

2.1.1 Resource Requirements

This section discusses the infrastructure required to integrate FileNet P8 platform with NetApp storage systems. This paper will briefly cover the hardware and software requirements for each of three possible FileNet P8 configurations.

Note that SnapLock fixed devices resides on a volume of the NetApp storage system using network protocols. NetApp recommends using the block protocol configuration (using either iSCSI or FCP) for installing and storing RDBMS application and data on NetApp storage systems. However, the recommendation changes while installing RDBMS application on UNIX platforms where either network or block protocols is ok (Discussion of installing RDBMS or content engine on UNIX platform is out of context for this report).

A P8 file store can reside on an OnTap volume, but not on a SnapLock volume. A P8 SnapLock fixed content device[1] [FCD] can reside on a SnapLock volume, but not on a NetApp storage system volume (While it is possible to create a FCD on a NetApp storage system non-SnapLock volume, it is not a valid configuration. This is due to the fact that contents of FCD do not reside on a SnapLock volume. Note that only SnapLock volumes maintain the retention setting requests of P8 server). Also, a file store can be created on a Filer in SAN mode or NAS mode, but a SnapLock FCD can only be created on a Filer in NAS mode.

To summarize, the following deployment options can be used to leverage a NetApp storage systems for P8 server:

- In SAN mode – deploy RDBMS data/log files and File Store Service transaction log files on the NetApp storage system(s).
- In SAN or NAS mode – deploy File Stores on the Filer.
- In NAS mode – use a SnapLock volume as a fixed content store.

[1] A SnapLock FCD is a multi-level directory structure created under a user defined root directory on a SnapLock volume.

Some examples:

File Store on a SAN

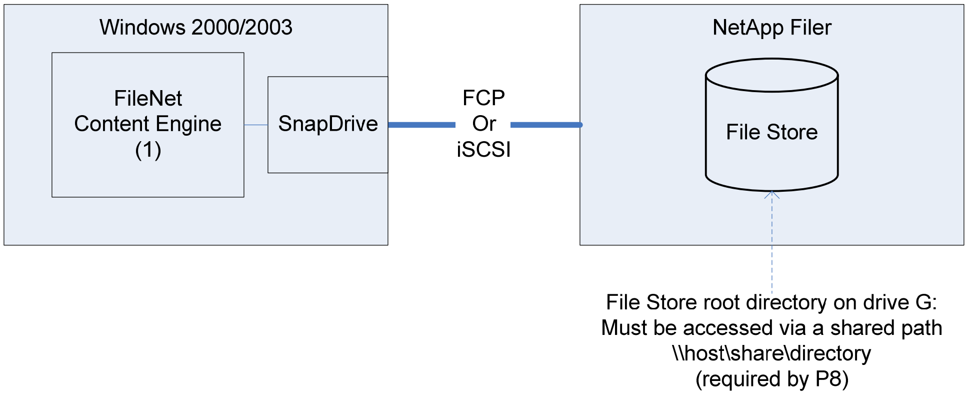


Figure 2: File Store on a Storage Attached Network Device

In this example above, a file store is located on a NetApp storage system in SAN mode. The root directory of the file store is located on a directly accessible [virtual] drive (say the 'G' drive), but P8 requires file stores to be accessed using a network share path (\\host\share\root-directory) - this is necessary to allow support for a second content engine computer (next example).

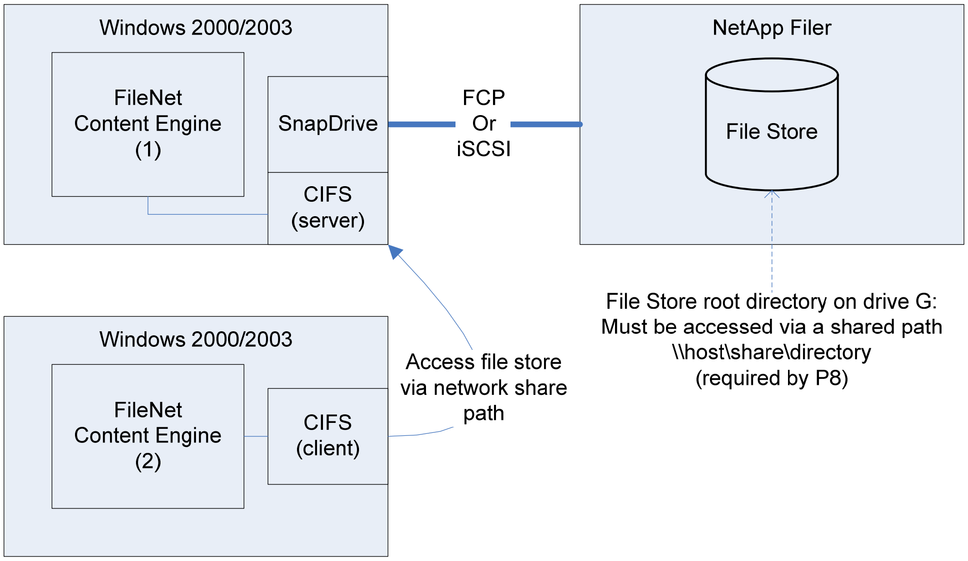

Windows 2000/2003
FileNet Content Engine (1)
SnapDrive
CIFS (server)
FCP Or iSCSI
NetApp Filer
File Store
File Store root directory on drive G:
Must be accessed via a shared path
\\host\share\directory
(required by P8)
Access file store via network share path
Windows 2000/2003
FileNet Content Engine (2)
CIFS (client)

Figure 3: File Store Access for a Second Content Engine on a SAN Device

The second CE server will access the file store directories via the shared path, the IO requests from CE server #2 will flow through CE server #1, since the share (in this case) is exposed by CE server #1.. Note that CE server #1 is also using CIFS to communicate with SnapDrive storage, since it is using a locally defined network path to access the file store volume. Note that CIFS protocol requirement with SnapDrive is only from storage management perspective such as LUN provisioning and Snapshot management. CIFS protocol is not required for data communication.

In order to use multiple servers to access the same file store (configured as LUN) requires a third party volume management tool such as Veritas Volume Manager. This application will ensure the data consistency while writing the data to the file store. Without using volume management application, such as Veritas Volume Manager, the configuration would corrupt the data. Generally sharing the same LUN by multiple servers is not supported and should not be configured. LUNs are often mapped to two (or more) hosts for clustering but the cluster ensures that only one of the hosts is actually talking to the LUN at any given time. There are some exceptions to this rule and that is clustered filesystem and Oracle RAC. In those cases the clustered filesystem or Oracle application manage the data access and caching to be sure that things are consistent. Multipathing is used manage multiple paths on each individual hosts. It does not span across multipath machines.

File Store on a NAS

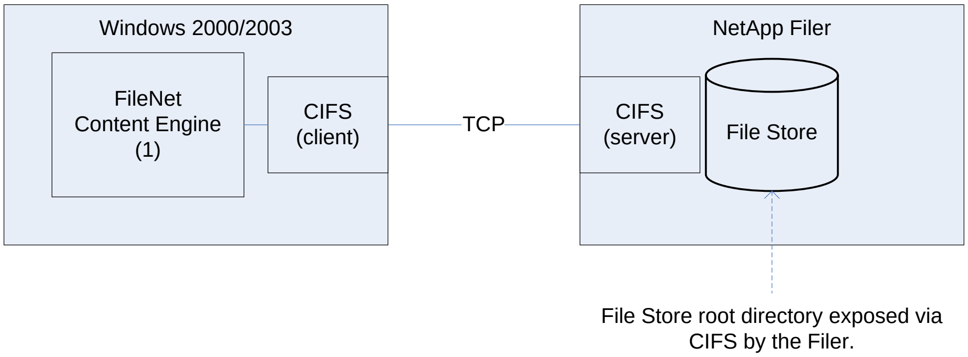

Windows 2000/2003
FileNet Content Engine (1)
CIFS (client)
TCP
NetApp Filer
CIFS (server)
File Store
File Store root directory exposed via CIFS by the Filer.

Figure 4: File Store on a Network Attached Storage Device

In this example the file store root directory is shared by the NetApp storage system (running in NAS mode) – i.e. the share is created on the Filer, and the Filer is the CIFS server. If a second CE computer is introduced, it will use the share exposed by the Filer (in contrast to the SAN example).

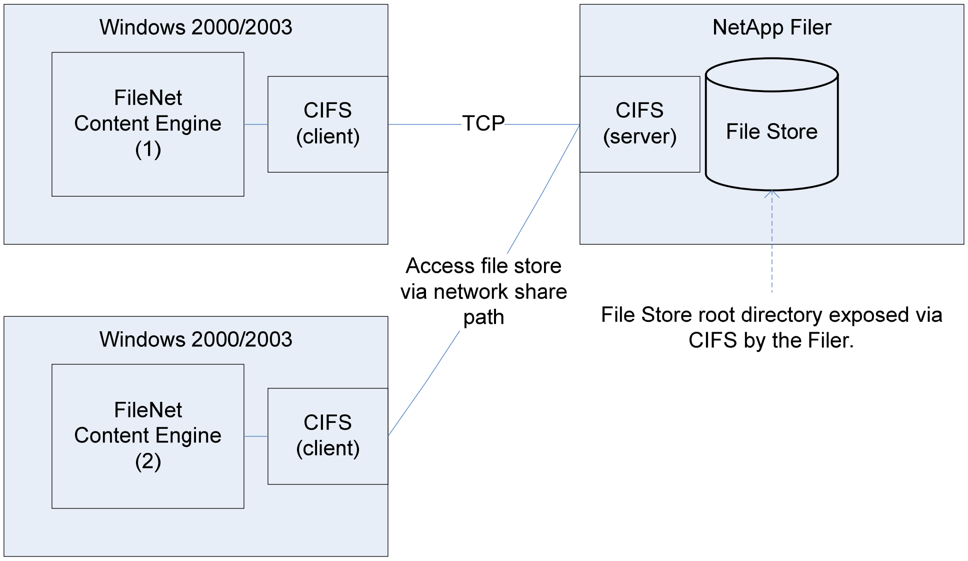

Windows 2000/2003
FileNet Content Engine (1)
CIFS (client)
TCP
NetApp Filer
CIFS (server)
File Store
Access file store via network share path
File Store root directory exposed via CIFS by the Filer.
Windows 2000/2003
FileNet Content Engine (2)
CIFS (client)

Figure 5: File Store Access from a Second Computer on a NAS Device

If a second CE server is introduced to the NAS configuration, it will use the share exposed by the NetApp storage system (in contrast to the SAN example, where the share is exposed by a CE server)

SnapLock Device on a NAS

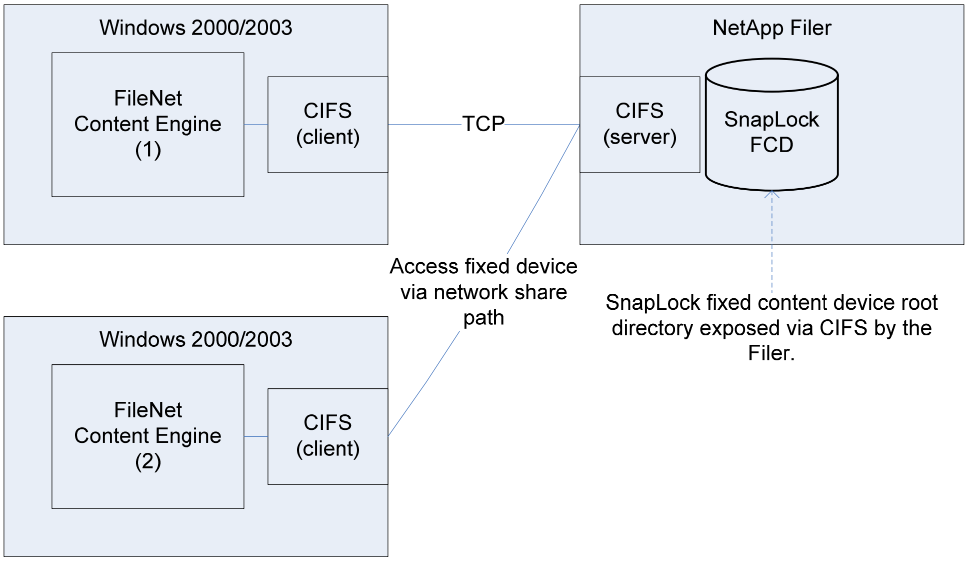

Windows 2000/2003
FileNet Content Engine (1)
CIFS (client)
TCP
NetApp Filer
CIFS (server)
SnapLock FCD
Access fixed device via network share path
SnapLock fixed content device root directory exposed via CIFS by the Filer.
Windows 2000/2003
FileNet Content Engine (2)
CIFS (client)

Figure 6: SnapLock Device on a Network Attached Storage Device

A P8 SnapLock FCD is defined on a NetApp storage system in NAS mode. The server configuration is identical to that of a file store using NAS. Note that a SnapLock Device does not support SAN mode, and hence SnapLockFCD must be configured in NAS mode only, using CIFS protocol (on UNIX platforms, NFS protocol supports SnapLock volume).

Resource Requirement for FileNet Baseline Configuration

Section 3.2 discusses the details of FileNet P8 platform configurations. In a baseline configuration, following hardware and software resources are required. At least four Windows servers are required to set up FileNet P8 baseline configuration in a production environment. Following is a list of the required FileNet P8 software components installed on each machine.

- Content Engine, Object Store Service, File Store service, Enterprise Manager, Publishing plug-in, and Content Federation Service for Image services installed on Windows 2000 or Windows 2003 server. This setup forms the content engine (CE) server. For backup and recovery purposes, recommended strategy is to install these software components and services on NetApp configured local disks. FileNet P8 platform requires file store configured as NTFS file system.
- On a separate Windows server, install the process engine component. This server runs process engine services in P8 platform environment.
- Rendition Engine servers will have Rendition Engine software installed on another Windows server. This server will run rendition engine services.
- In case the image services configuration is involved, this service runs on a separate server. This configuration may need additional infrastructure requirements.
- Application Engine server serves as a presentation layer to the clients with the FileNet P8 system. There must be at least one application between the Internet/intranet clients. This runs the application

engine. In a larger environment, there could be multiple application engines running on different servers.

- FileNet P8 platform requires a relational database instance running on a server within the network. Note that SQL Server may run on a dedicated server or on the server running content engine services. If the database engine is running locally on the content engine server, it becomes a local database instance as opposed to a remote instance. Running the database instance on a dedicated server depends on the system workload and performance considerations. On our test setup, we installed SQL Server on the content engine server and used it as a local database instance.
- In addition to this, additional client workstations or desktop clients access P8 platform components and services over Internet or intranet environment.
- NetApp provides the unified storage capability by supporting multi-protocol feature with both SAN and NAS configurations on the same storage system. Before attempting to install the software, this paper recommends completing the appropriate local storage configurations using NetApp storage system. This includes the requirement to configure virtual disks by using storage management tools such as SnapDrive with SAN or IP-SAN architecture. To install fibre attached host kit, refer to the NetApp SAN and IP-SAN documentations, SnapDrive support matrix, installation, and configuration guides, available at our customer Website.
- In a FileNet P8 platform configuration, generally one or more NetApp storage systems are used. FileNet P8 platform requires the following NetApp configurations:

SAN or IP-SAN based configuration for configuring local disks for installing Content Engine, process engine, application engine, rendition engine, and optionally image services software components on NetApp storage systems.

Host Attached Kit with supported host bus adapter and other supported components.

Storage capacity to meet the FileNet P8 platform storage requirements.

Configuration of SnapLock volume either on the same NetApp storage system or on a separate NetApp storage system.

Enable the appropriate NetApp product licenses on all NetApp storage systems. This includes licensed products such as SnapDrive, CIFS, FCP, SnapLock, etc.

Configuration of SnapLock volume and setting the retention period require professional help. This paper strongly recommends seeking professional help in configuring NetApp storage systems with SnapLock. Test this SnapLock configuration on a test or simulator environment to avoid any serious configuration errors. Contact the NetApp sales team to get the access to simulator software. Content Engine supports any NTFS file system for storing the content and NetApp SnapLock for storing and managing the fixed content devices. Fixed content devices supported by SnapLock address the compliance requirements in FileNet P8 platform configurations. WORM Storage on Magnetic Disks Using SnapLock Compliance and SnapLock Enterprise document provides additional information SnapLock product. Current releases of NetApp storage solution allows both types of SnapLock features on the same NetApp storage system.

Baseline configurations with optional components requiring additional Windows servers are required. Capture workstation runs the capture FAX import tasks, eForms designer workstation supports FileNet eForms designer, Capture workstation to capture scanning tasks, and process simulator and process analyzer server are a full-fledged system.

In testing our demonstration configuration, a single Windows server hosts the required P8 components. This paper recommends image services installed on a dedicated system. This paper also recommends avoiding collocating records manager on the same server as content or processing engine.

Developer's configuration includes several workstations along with a server for P8 components, and another server for running image services.

2.1.2 SnapDrive Software Installation

SnapDrive supports both Fibre Channel and IP based iSCSI protocols. SnapDrive allows ease of dynamic storage management. Refer to SnapDrive for Windows documentation for additional information on SnapDrive software.

For installing SnapDrive software, refer to SnapDrive installation and Administration guide. This paper will not discuss the details of SnapDrive installation procedure.

2.1.3 Microsoft SQL Server

FileNet P8 platform requires Microsoft SQL Server 2000. In a large FileNet P8 environment, a dedicated SQL Server on a separate Windows server configuration helps to address the performance and management needs. Use SnapDrive to address storage management needs. SnapManager® for SQL Server allows the database to perform backup and recovery easily. Using SnapManager for SQL Server and SnapDrive, you can have a consistent backup and restore the data if required.

In a local database configuration, install SQL Server on either Process Engine Server or Content Engine Server machine. Installing SQL Server on a different server provides the remote database capability. If the SQL Server installed on the machine where CE, PE or RE servers are installed, then it is considered as local database instance. In the remote database configuration environment, note the following information before attempting to install FileNet P8 software:

- SQL Server installed as local database or on a separate server (remote database)
- PE, CE, RE and Publishing Plug-in server, supports remote SQL Server databases
- FileNet Enterprise Manager and RE servers manage remote SQL connections using Microsoft Data Access Component (MDAC)
- SQL Server must be in the same Active Directory forest if the Windows authentication method used
- Complete the MSDTC and COM+ setup

During the test setup, we used a SQL Server 2000 SP4 and created data and log devices on SnapDrive configured virtual disks. After the system configuration check, use the FileNet setup program to start the installation process. Selecting the SQL Server authentication mode that specifies the security used when connecting to SQL Server is important. There are two authentication modes. They are Windows authentication mode and mixed mode, which includes the Windows authentication as well as SQL Server authentication. In our test setup, we selected Windows Authentication mode. It may be relevant to select Dictionary order, case-insensitive collations settings during the SQL Server installation. Verify and note down the server type, SQL Server instance and the authentication mode. Installing SQL Server may require a system reboot for the change to be effective.

2.1.4 Domain Users Account Information

FileNet P8 configuration requires a Windows Active Directory (AD) domain that includes a domain controller and Windows system accounts for content services. Before creating the user groups and user accounts, installing a supported authentication provider such as Windows Active Directory, Sun™, or Novell is a requirement. This paper recommends having non-blank passwords in FileNet P8 platform environments. Active Directory authentication, FileNet P8 supports only security groups, not distribution groups.

For Content Engine and Process Engines have a different requirements and some of the key points are listed below.

- The Content Engine uses both Operating System user/group accounts and Authentication Provider user/group accounts.
- The OS accounts are used to secure OS resources, like a file store or SnapLock FCD. The security settings on these resources prevent unauthorized access at the OS level (i.e. someone trying to browse to a content file).
- CE to secure CE resources, like documents in an object store, uses the Authentication Provider accounts. The security settings on these resources are only honored/enforced by P8 (the OS doesn't know anything about a P8 document). Note that these accounts are not intended to have an impact on OS resources, but there can be confusion when the Authentication Provider is Active Directory, since these are also OS accounts (we always logically separate them).
- There are three important OS accounts:
  a) Content Engine Servers group (normally system generated)
  b) FNCE_<machine> user (normally system generated)
  c) Content Engine installer user

- Content Engine Servers group – this account must have full control access to all OS resources used by the CE (for example, the root directory of a file store must grant full control access to this account).
- FNCE_<machine> user – this is the user account that all Content Engine services run under, and must be a member of the Content Engine Servers group (the group is granted access to resources, the machine user account gains access via group membership). Note that the machine account is a domain account, but is normally named differently on each CE computer (that way the installer doesn't need to know the password for the account, it can just reset the password and change it on the local CE services as needed – without impacting other CE computers).
- Content Engine installer user – this is the user that logs on and installs the product, creates file stores and SnapLock FCDs. This user must have full control permissions on OS resources used by the CE.

Content Engine supports Microsoft SQL Server, Oracle®, or DB2 database servers. MS SQL Server security login is required to enable the system to create content engine objects. This user must have system, security, disk administrator, and database creators' server roles with the database access permission to public and db_owner for all object store databases. Similarly, Oracle and DB2 require a user account created with appropriate access permissions. This user requires the local administrator role privilege and a member of domain users. Windows Active Directory group and users under group are required for each machine on which Content Engine is installed. Default user created will be FNCE_contentengineservername. On our test setup, a user called FNCE_IBMX335-SVL62 was created by default. GCD Administrator role enables adding marking, AddOns, and FileNet P8 domain objects. On our test setup, we created FileNet P8 domain called P8CE. P8Apache user account runs the Apache2 service as LocalSystem. Object store administrator's role has full control access to an object store and this helps to administer on day-to-day basis. Rendition Engine uses <SQL Login> and a Rendition Engine administrator's account. A Windows domain user account is a member of local administrators group on all Rendition Engine servers. On our test setup, we used a domain called IOP. Following FileNet P8 platform related users and user groups are required to install and configure FileNet Process Engine services.

FileNet P8 platform requires the following user groups and users.

Groups	**Users**	**Description**
Administrators	Administrator	To Install Process Engine Software
fnadmin, fnusr , dba	Fnsw , oracle	'oracle' user is required for Oracle Database installation
<Process Engine Administrators Group>	<process engine service user>	Users and groups are required to designate as members of the Application Engine administrator role

Figure 7: FileNet P8 Platform User and Group Information

2.1.5 Mapping the Network Share

FileNet Content Services support Windows NTFS file system for archival destination. On Windows server, this includes local disks, configured virtual disks with or without SnapDrive using NetApp storage systems or a network-mapped share. Fixed-content object store using SnapLock volume requires a network mapped share. If the network share is used, make sure to have the network connectivity for the content engine server. For this purpose, configure the network connectivity between the FileNet P8 platform server and NetApp Storage system(s). Once the network connectivity is established, verify the storage volume configuration on the NetApp systems. Object stores require NTFS file system. Data ONTAP software from NetApp provides a greater flexibility in storage configuration in defining and configuring volume sizes. This architecture allows scaling the storage by allowing a particular volume to be expanded or shrunk dynamically.

The Content Engine requires all file stores and SnapLock FCDs be accessible via integrated Windows security, meaning that:

a) The NetApp storage system must be joined to the Windows domain that the Content Engine is deployed in.
b) Any share on the NetApp storage system that is used by Content Engine (file store or SnapLock FCD) must grant full control access to the Content Engine Servers[2] Windows Active Directory security group.
c) The share does not need to be mapped on any Content Engine computer - each instance of the Content Engine can access the share via a host\share style path.

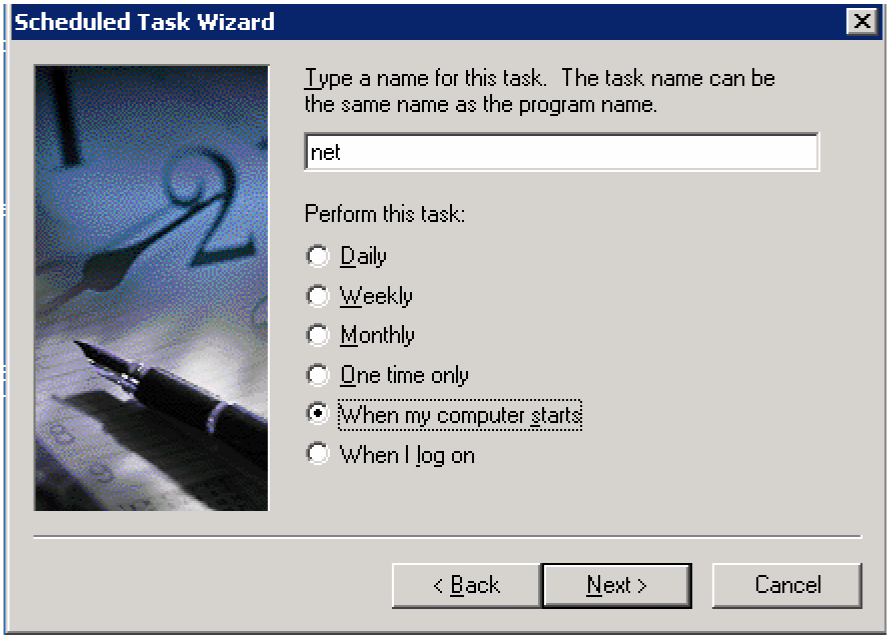
Enabling CIFS license and CIFS setup is a prerequirement to create a network share. On our test setup, we used two storage systems, one FAS3050C system, and another R200 storage system. On each system, we created the necessary CIFS Shares. In our test setup, we created P8 fixed-object stores on network shares created on SnapLock volume(s).

[2] Refer to Section 2.1.4 for user and group accounts information

This section provides some additional information about network-mapped drive connectivity even when all users log out on Windows server. Maintaining the continuous network connectivity to the network share may address data access capability to the content server.

For Windows XP/2000 and Windows Server 2000/2003, create a Scheduled Task that executes with a schedule of "At System Startup". The Run As account will need to be an account that has permissions to the remote share. This will allow you to map a drive to the remote machine at startup without anyone logged in.

The "Run" command in the scheduled task can be as simple as "net use H: \\servername\sharename". To map multiple drive mapping, this paper recommends executing batch files. Examples of the Task and Schedule Tabs for the Scheduled Task are shown below. To schedule a Windows task to automapping a network share, open Windows task manager and select the new task option, either the UNC path or a drive letter assigned depending on the ‘net use’ command. Alternatively, you may use GPO script to auto map the network shares without using any login script. This works only on Windows 2000 and Windows 2003 platforms and not on Windows XP clients. On our test setup, we created a Windows task schedule by specifying ‘net.exe’ tool. Specify the login user credentials for mapping the specified network share.



Scheduled Task Wizard

Type a name for this task. The task name can be the same name as the program name.

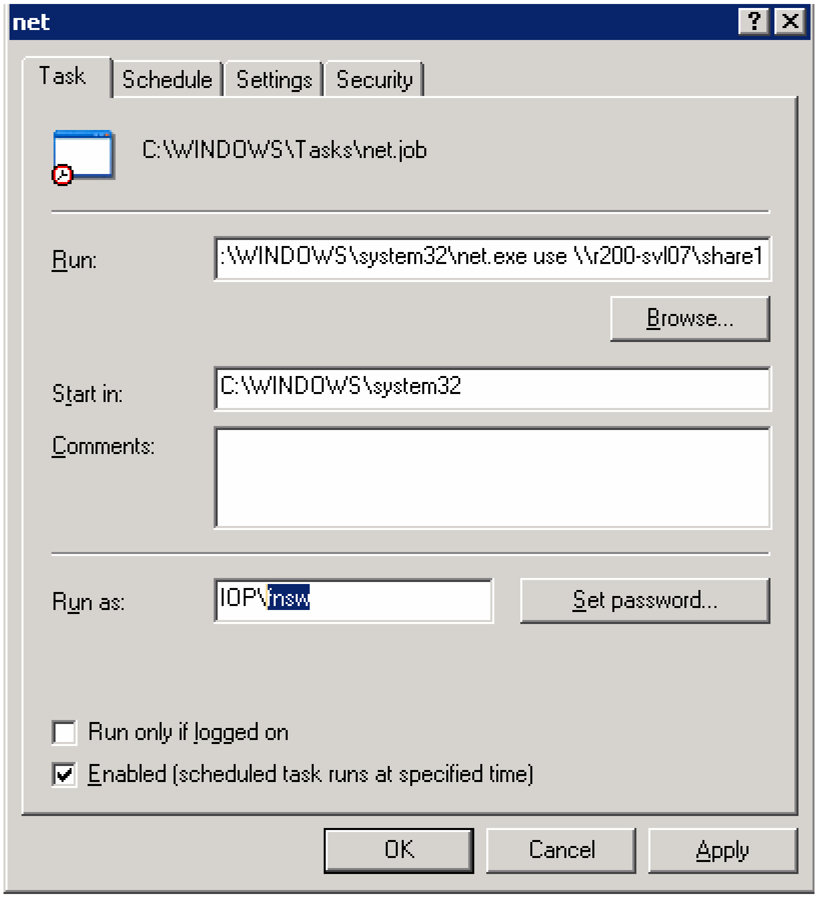
net

Perform this task:

○ Daily
○ Weekly
○ Monthly
○ One time only
● When my computer starts
○ When I log on

Figure 8: Windows Task Scheduler

On our test setup, we created a Windows task scheduler to map a network share every time the content server starts. Following figure demonstrates the procedure to map a network share.



C:\WINDOWS\Tasks\net.job

Run: :\WINDOWS\system32\net.exe use \\r200-svl07\share1

Start in: C:\WINDOWS\system32

Comments:

Run as: IOP\nsw

☐ Run only if logged on

☑ Enabled (scheduled task runs at specified time)

Figure 9: Automatic Mapping of Network Share

This procedure will enable FileNet P8 components to access the data on the network share even when users are not logged in to the system.

2.1.6 Configuring Write Once, Read Many Storage Using SnapLock Software

Content engine manages content and user-defined business objects. Content and business objects include electronic documents, Web content, records, folders, simulation scenarios, and other types. An object store is a repository for storing contents such as documents, folders, and business objects. The object store service is responsible for adding new contents to a fixed content store and contents via the file. Fixed content provider integrates with Image Services and NetApp SnapLock storage solution for managing the content in the specified repositories.

Corporations must successfully archive and retain the content in its state as a read-only for the specified retention period. To achieve this requirement, a volume with SnapLock license is configured. On the NetApp storage system, appropriate SnapLock product license is enabled. Currently there are two types of supported SnapLock features. SnapLock license supports a version of compliance volumes where the content of the files remains in immutable state until the retention period expires. Another version is known as SnapLock for Enterprise, and the storage administrator will have the control over that volume. Based on the company policy, configure the appropriate SnapLock volumes. Data ONTAP supports both types of SnapLock licenses simultaneously on the same NetApp storage system. For detailed information on the support matrix, visit the NetApp customer support site. Refer to the technical paper on SnapLock to obtain additional information about SnapLock. Care must be taken while creating a SnapLock volume. This paper strongly recommends documenting the retention policy and the storage configuration. Storage administrators in consultation with their retention policy must complete SnapLock configuration. Following command syntax is an example to create a SnapLock aggregate. All volumes created under this aggregate inherit the properties of the hosting aggregate. It is mandatory to define a retention policy and seek professional help while configuring SnapLock volume(s). Following is a syntax of creating a aggregate on NetApp storage system.

```
aggr create <aggr-name>
    [-f] [-l <language-code>] [-L [compliance | enterprise]]
    [-m] [-n] [-r <raid-group-size>]
    [-R <rpm>] [-T {ATA | EATA | FCAL | LUN | SCSI}]
    [-t {raid4 | raid_dp}] [-v] <disk-list>
```

Any volume created hosting a SnapLock supported aggregate becomes a SnapLock supported volume. A sample command procedure to create a SnapLock shown below.

```
Netappsystem> aggr create agg1 –L compliance –r 14 –t raid_dp 10
```

Above command creates a SnapLock compliance aggregate called ‘aggr1’ with a raid group size of 16 disks, double parity with 10 disk spindles. Additional disks added as and when required. Once the hosting SnapLock aggregate created, new volume(s) added by hosting on this type of aggregate. Command to add volume as shown below. Note that the following command syntax applies to FlexVol type of volumes. Traditional volumes use, ‘-L’ option with the ‘vol create’ command syntax.

```
vol create <vol-name>
   { [-l <language-code>] [-s {none | file | volume}]
     <hosting-aggr-name> <size>[k|m|g|t]
```

2.2 Preinstallation Tasks

FileNet P8 setup requires the following preinstallation tasks for successful installation and configuration of the server. This paper assumes that the necessary NetApp storage systems configured and storage space available. Earlier sections covered some of the preinstallation tasks. For completeness of information, this section details the tasks that need to be completed to meet the preinstallation tasks. The tasks listed below help to install and configure the FileNet P8 platform successfully.

- Plan the Installation of P8 platform
- Obtain the P8 documentation and software updates
- List the preinstallation tasks
- Prerequisite Tasks
- Postinstallation Tasks

This section attempts to provide all the information about preinstallation tasks required for successful FileNet P8 platform components.

<u>Set up and configure NetApp storage systems</u>

Complete preinstallation checklist to verify that storage resources are configured and available. This includes the installation and setup of NetApp storage systems, installation of additional NetApp software products such as SnapDrive, and host bus adapter kits. FileNet P8 platform components software installation requires the virtually configured local disks for NetApp storage systems. Installing all components of FileNet P8 platform on NetApp storage system(s) allows simpler backup, recovery, and data replication capabilities. This may require configuring the virtual disks on all FileNet P8 platform components machines such as every content engine and process engine server.

Content Services server requires the host name resolution for all P8 platform servers. Edit ‘hosts’ file to include the hostname and necessary Internet protocol (IP) address. On Windows server, this file is located under \Windows\system32\drivers\etc folder. Hosts file entry is especially true with the Image Services (IS) configuration.

Verify that MTDTC and COM+ services are installed and the services enabled. This is a prerequirement for FileNet P8 platform configuration. Installing these services may require Windows media kit.

Verify Microsoft Internet Information Service (IIS) us installed and enabled. IIS services are required for WebDAV application.

Note that Rendition Engine and Publishing currently support Windows 2000 platform. For latest platform support, this paper recommends checking with FileNet support site.

FileNet P8 platform requires servers to have static IP addresses and configuring the TCP/IP settings.

Another Requirement is ensure the availability of P8 required port numbers for communications.

All Windows-based P8 servers must be configured in the Windows domain.

FileNet P8 3.5.0 release does not support multi-forest configurations and requires at least one Windows domain configured.

P8 environment requires a Windows domain controller and P8Apache user account.

Determine the FileNet P8 components to install on Windows domain such as all components of Content Engine, FileNet Enterprise Manager, SQL Server, and Rendition Engine.

Once Content Engine Servers are installed and configured, their names cannot be modified.

LDAP Authentication provider such as Active Directory, eDirectory or Sun Java™ System Directory Service is required.

Check user and group account privileges such as ‘fnsw’ as a local user account created during PE setup.

Logons to P8 applications cannot share user credentials and installation user has local administrator privilege.

Complete Windows authentication configuration.

Configure either the local or remote database engine. Some of the configurations available use a shared database engine for Content Engine, Process Engine, and Rendition Engine. Another configuration option uses databases of their own for each CE, PE, and RE service. It is necessary to create the SQL login for content engine service with appropriate user privileges. These privileges include security admin and database creator roles.

Content engine, process engine and rendition engine can share a single database instance. On Windows 2003 SP1 platform in a FileNet P8 environment, follow the procedure listed below.

- Configure or verify that a Windows 2000 or 2003 for the P8 environment regardless of authentication provider.
- Microsoft Distributed Transaction Coordinator (MSDTC) and COM+ must be configured and enabled.
- Boot drive partition where Windows 2003 installed must be NTFS file system.

- Process Engine software release of 3.5.0a or later version required to install PE.

Applying the 3.5.x service upgrades FileNet P8 platform components. This means, FileNet P8 3.5.0 version of the software must be installed before upgrading to later releases of 3.5.x.

Complete list of user and group roles and responsibilities required to install, configure, and maintain a FileNet P8 system.

Be aware of FileNet P8 High Availability options to use clusters, farms, and other high-availability software and hardware configurations.

On each Windows OS-based FileNet P8 server, the Windows host file must contain the Windows server name and Internet Protocol (IP) addresses of all servers with which it will communicate including database server. On UNIX® based FileNet P8, /etc/hosts file must contain the information about the servers including the remote database server.

If a firewall environment is used, ensure the necessary port is available for communication before starting the P8 installation.

FileNet P8 servers are configured to have static IP address.

TCP/IP settings are configured on all servers and Enterprise Manager Clients.

FileNet P8 environment requires at least one Windows domain configured, regardless of authentication provider.

Best practice is to include all Windows based FileNet P8 servers in the Windows domain. Multi-forest configurations are not supported with FileNet P8 3.5.x releases.

Here is a list of tasks that need to be completed for a successful installation and configuration:

- Install and configure a Windows domain for Content Engine.
    - At least one Windows domain must be configured for the FileNet P8 environment regardless of authentication provider.
    - Verify boot partition is NTFS on Windows platform.
    - Windows domain controller must have a static IP address.
    - DNS server component is installed and configured properly.
    - Domain controller is set up and configured.
    - Network configuration settings such as TCP/IP, DNS, subnet mask are verified.
    - Domain controller, Content Engine, FileNet Enterprise Manager, servers that contain remote Content Engine File Store and File Store Service, remote Content Cache Service, Microsoft SQL Server with Windows authentication must be located on machines that are members of the Windows domain.
    - Authentication provider configuration procedure must be completed.
- Configure FileNet P8 Platform authentication with Active Directory, or Sun Java System Directory Server or Novell eDirectory configuration.

    - In mixed-mode Windows domains, user members of Domain Local Groups are recognized only if Content Engine is installed on the Domain Controller. This may result in degraded performance.
    - DNS forwarders provide external DNS lookup functionality.

- Create FileNet P8 Platform groups and users.
    - All FileNet P8 environments require a Windows Active Directory domain/forest, including Windows domain controller and Windows accounts that are used for Content Engine services.
    - Content Engine requires a SQL Login. MSSQL Server Security Login required to enable the system to create Content Engine object stores when requested by administrators. Oracle user is required by Oracle Database server; DB 2 user account is an operating system user on the database server in DB2 environment.
    - Windows local Administrator role allow to install Content Engine and create a FileNet P8 domain or adding a new server into an existing P8 domain.
    - Content Engine servers group is the Windows Active Directory group and user accounts used on each machine on which Content Engine installed.
    - Administrators’ role who can add or remove FileNet P8 domain objects.'
    - Authentication Service user role to connect and search the directory server when Sun or Novell authentication mode used.
    - IIS user for Content Engine WebDAV role.
    - P8Apache user account that logs on and runs the Apache2 service as LocalSystem.
    - Process Engine requires the local administrator role to install the software.
    - Groups – fnadmin, fnusr and database administrators group such as dba.
    - Users – fnsw and Oracle user if Oracle Database configuration used.
    - <FNRE_Admin> is a Windows domain user account that must be added to the local administrators group on all Rendition Engine servers.

- Install database server for Content Engine and Process Engine. Supported database servers are Microsoft SQL Server, Oracle and DB2.
    - Configure MSDTC and COM+ on each Content Engine machine and Microsoft SQL Server machine.
    - Install IIS for Content Engine WebDAV support if it is not already installed.
    - Enable Windows 2003 IIS when acting as a WebDAV client.
    - Microsoft SQL Server must be in the same Active Directory forest if the Windows authentication mode is used.
    - Content Engine may have either Windows Authentication or Mixed-mode configurations.
    - Process Engine requires Mixed mode.
    - Rendition Engine requires Mixed mode.
    - Content Engine, Process Engine, and Rendition Engine components may share the same MS SQL instance.

    - Note down the Server name, instance and dedicated database name, dedicated file group and TCP/IP port number assigned.
    - Configure SQL Login for Content Engine.
- Install database client software that requires access to database engine.

2.3 FileNet P8 Architecture

In this section, we discuss briefly the FileNet P8 System architecture and product integration methods with NetApp storage systems. FileNet P8 platform include back-end services, development tools, and applications to address enterprise content and process management requirements. FileNet P8 platform addresses enterprise-level scalability issues. It has built in flexibility to manage the content efficiently while resolving the complex business processes. FileNet P8 architecture offers scalable and highly available configuration that is a basic requirement in enterprise level configurations. It enables you to streamline and automate business processes and manage all types of contents. FileNet P8 architecture offers robust record management capabilities. Content Engine, Process Engine, Application Engine, and Rendition Engine components offer the enterprise content management solution.

FileNet P8 architecture Additional components included in P8 platform listed below.

- Records Manager
- eForms for P8
- Capture
- Email Manager
- Team Collaboration Manager
- Web Content Manager
- P8 Portlets
- Process Analyzer
- Process Simulator
- Image Manager
- Content Federation Services
- Image Services Resource Adapter

FileNet P8 architecture allows you to integrate its document management software Image Services to make it a truly an enterprise content management solution. Following diagram clearly explains the architecture of FileNet P8 platform environment.

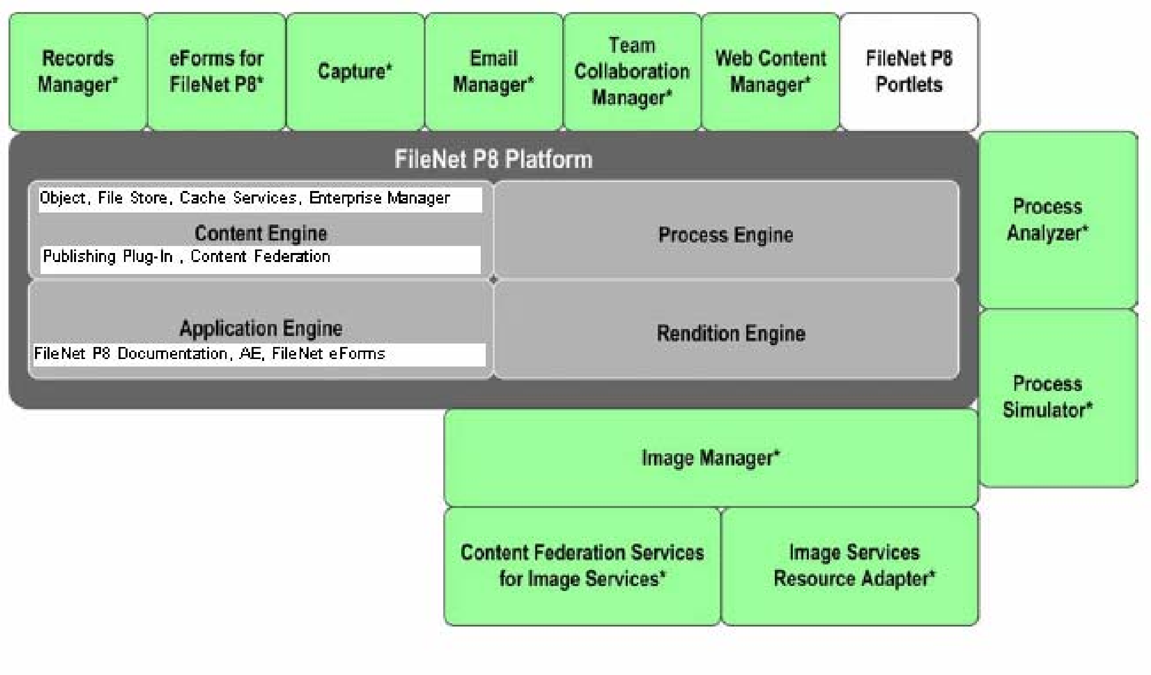

Records Manager*
eForms for FileNet P8*
Capture*
Email Manager*
Team Collaboration Manager*
Web Content Manager*
FileNet P8 Portlets
FileNet P8 Platform
Object, File Store, Cache Services, Enterprise Manager
Content Engine
Publishing Plug-In , Content Federation
Process Engine
Application Engine
FileNet P8 Documentation, AE, FileNet eForms
Rendition Engine
Process Analyzer*
Process Simulator*
Image Manager*
Content Federation Services for Image Services*
Image Services Resource Adapter*

Figure 10: FileNet P8 Architecture

FileNet P8 platform includes Content Engine (CE), a service that provides software services to manage content and user-defined business objects. CE manages a broad range of enterprise content and objects including electronic documents. Object store, library services, content-related services, and WebDAV Provider are some of the services and components of Content Engine. Enterprise Manager is a Microsoft Management Console (MMC) snap-in application to allow the FileNet Administrator to manage CE services. Process Engine (PE) provides software services for managing all aspects of business processes (workflows). Application Engine (AE) is P8 platform component that hosts the Workplace Web application, Java applets, process router, and application development tools.

2.4 NetApp Storage Systems

It is important to plan FileNet P8 platform architecture regarding the storage configuration. FileNet P8 platform environment requires either local disks or virtual local disks for installing the SQL Server and P8 platform components such as content engine services. Either SAN or IP-based SAN accomplishes the requirement. Installing NetApp software tools such as SnapDrive will ease the storage management issues. SnapDrive tool allows storage management tools such as quick backup and recovery of data in the FileNet P8 platform environment. The necessary software and hardware configuration topics are discussed in earlier sections. For details, refer to NetApp support Web site. In our test setup, we used NetApp storage systems to configure local disks on both content engine server and to store object store repositories. For archival destination, we used a FAS3050 cluster configuration and a near-line storage system R200 to archive the content.

3. Configuration

Currently FileNet P8 platform supports only Windows platform. For UNIX platform and latest support matrix, refer to FileNet documentation. Before installing FileNet P8 components, make sure that configuration of Operating System and NetApp storage systems is complete. FileNet supports NTFS volume and NetApp SnapLock enabled volume on Windows platform. In a network share configuration for storing the object store for repositories, ensure the network connectivity for storage availability. This section briefly discusses the configuration of the operating system, FileNet P8 platform, and NetApp storage systems.

3.1 Operating System Information

On Windows platforms, P8 supports Windows 2003, Windows 2000 with SP3 and Windows 2000 Advanced Server with SP3 platforms. On our test setup, we used two Windows 2003 SP1 server and Windows 2000 servers. Our test setup followed the baseline configuration with three P8 components such as CE, PE and RE servers installed on a separate Windows server. Installing SQL Server on a separate server may allow improved performance of P8 platform.

3.2 FileNet P8 Platform Configuration Information

It is required to install and configure TCP/IP on the Windows machine. This computer should have Internet protocol (IP) address registered with Domain Name System (DNS). For performance reasons, this paper recommends a minimum of 2GB of main memory. It is also important to ensure SQL Server access to FileNet Content Server.

This type of configuration includes FileNet Image Services (IS) server component to be a part of FileNet P8 baseline configuration. On demonstration configurations, all P8 components installed on a single server serve the purpose. However avoid collocating the Records manager on the CE and PE server. P8 Email manager component manages the email content in the P8 architecture. Email management application could be running Exchange server or Lotus Notes. If these applications use NetApp storage systems, refer to NetApp technical library for additional details to install and configure the storage systems.

FileNet P8 supports Data ONTAP software for Content Services. In order to support compliance data with SnapLock, FileNet P8 requires version 3.5.2 or later releases. Ability to remove the retention expired items from SnapLock volume is a supported feature with fixed content store repositories with SnapLock volume configuration.

As discussed earlier, there are four P8 configurations available and they are:

- Baseline configuration where Content Engine, Process Engine, Rendition Engine and IS Servers are installed on each Windows server and networked to Web/Application Server and then to client application over the Internet/intranet connectivity.
- Baseline configuration with optional components allows user to utilize the functional expansions components in addition to core P8 platform components. Following figure demonstrates the baseline configuration with optional components in FileNet P8 platform environment.
- Developer Configuration with various developer workstations connected to content server and Image servers. In this configuration, content engine and process engines shared among the development workstations.
- Demonstration configuration involves a single server. Currently Rendition Engine installed on Windows 2000 server and not Windows 2003.

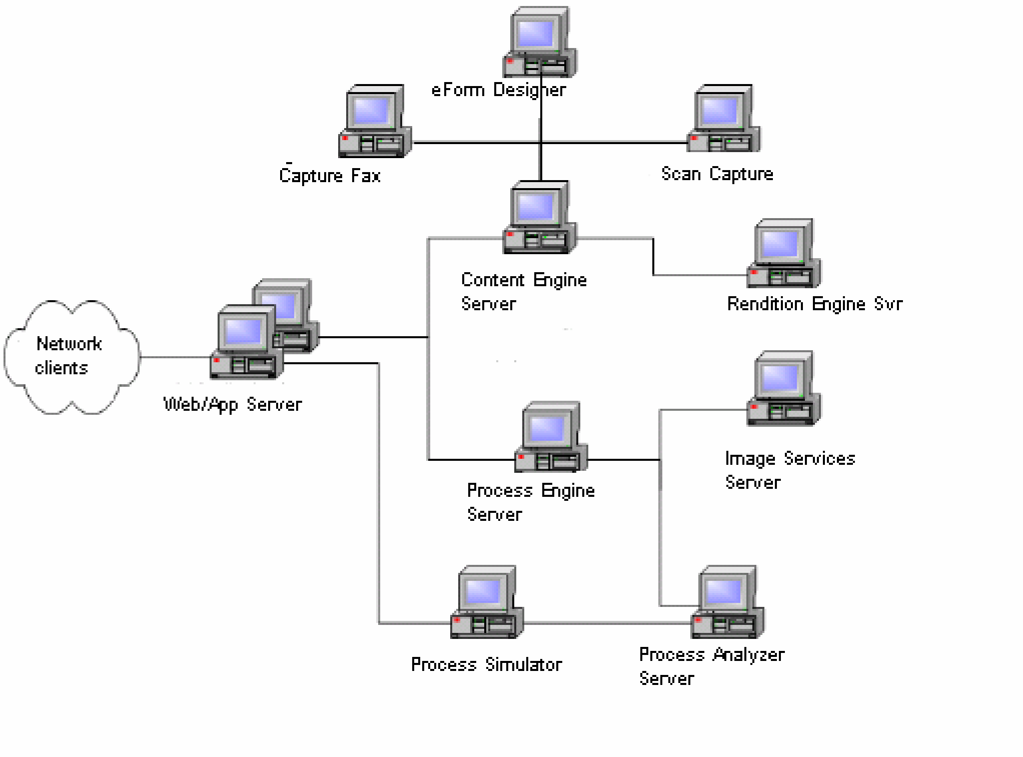


Figure 11: Baseline Configuration With Core Components in FileNet P8 Platform

3.3 The FileNet P8 User Account

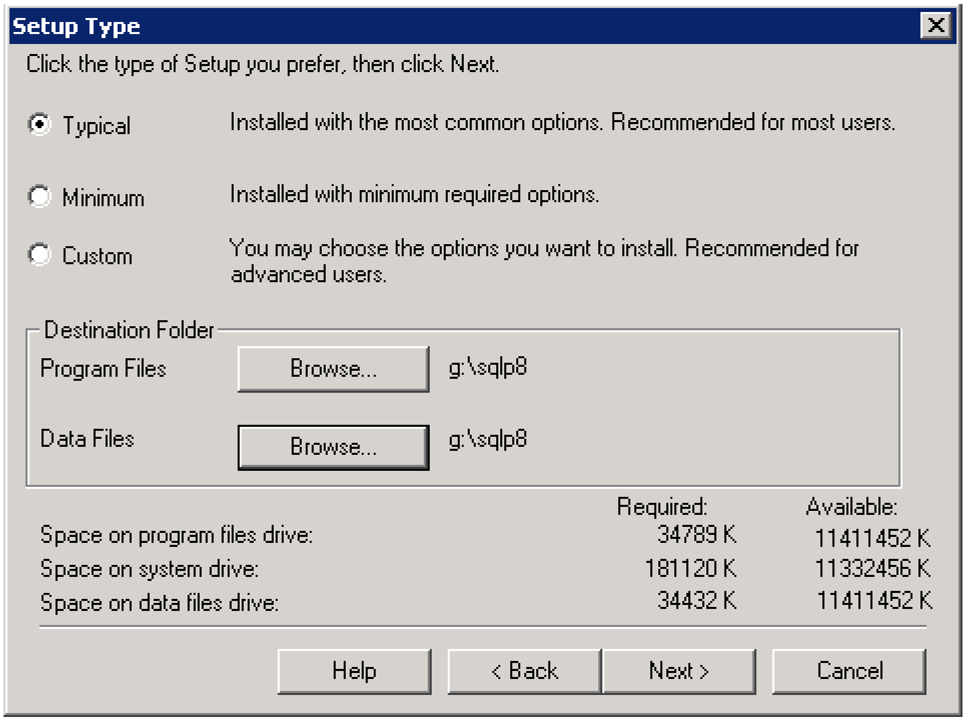
FileNet P8 configuration requires a specified user groups and users account created with appropriate permissions to access the Windows server operating system. Section 2.2 discussed in detail the user groups and user account requirement. On our test setup, we created use 'fnsw' and 'sql1' and added 'fnadmin' group. SQL Server name on our test setup is IBMX335-SVL61 with the same instance name, dedicated database name of CEdb and the dedicated filegroup of P8db_fg.

3.4 SnapDrive Software Installation and Configuration

SnapDrive tool eases storage management on Windows server. It integrates with Microsoft Windows Management Console utility. Using this tool, configure the required local drives and complete the storage configuration as needed.

3.5 Microsoft SQL Server Configuration

Enterprise Vault™ requires Microsoft SQL Server installed and configured properly. SnapDrive configured NetApp storage system's virtual local disks support SQL Server. Section 2.1.3 described the details about Microsoft SQL Server installation. On our test setup, we installed SQL Server on SnapDrive configured local drive as shown below.



Setup Type

Click the type of Setup you prefer, then click Next.

● Typical — Installed with the most common options. Recommended for most users.

○ Minimum — Installed with minimum required options.

○ Custom — You may choose the options you want to install. Recommended for advanced users.

Destination Folder

Program Files g:\sqlp8

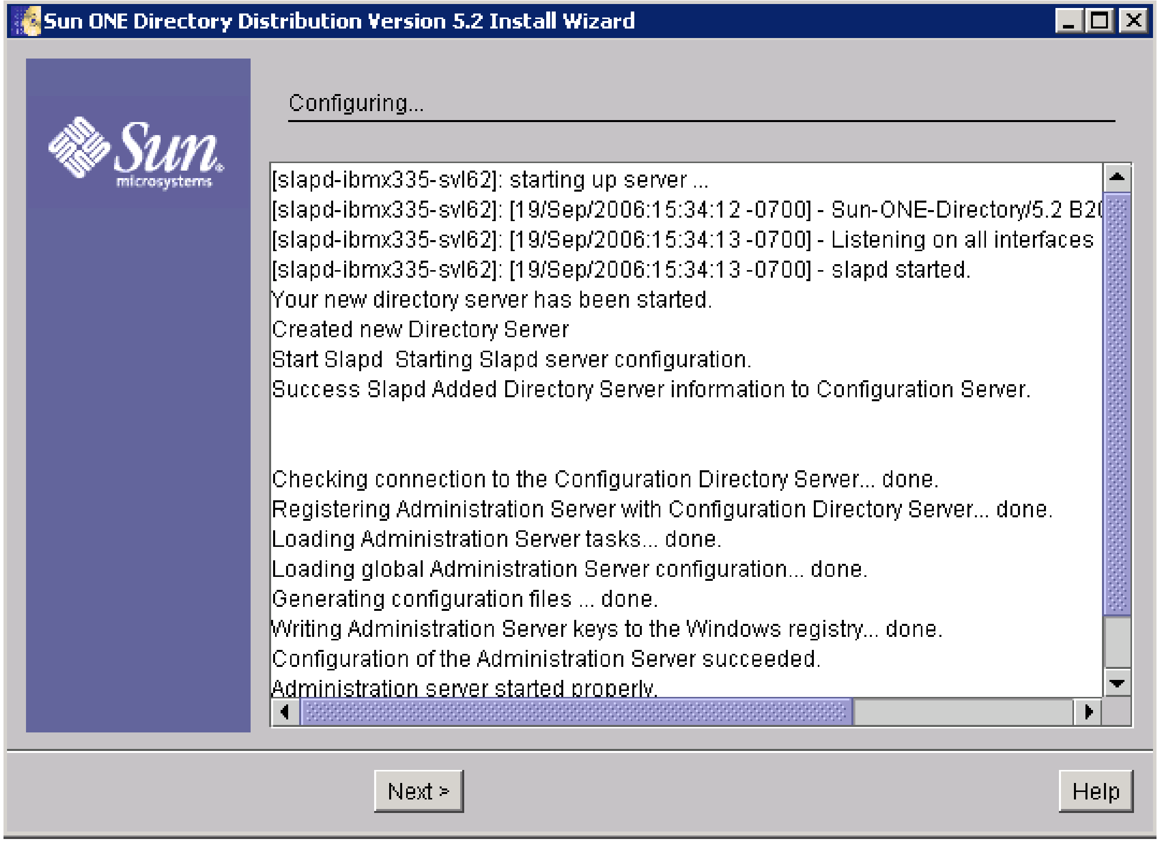
Data Files g:\sqlp8

	Required:	Available:
Space on program files drive:	34789 K	11411452 K
Space on system drive:	181120 K	11332456 K
Space on data files drive:	34432 K	11411452 K

Figure 12: SQL Server Installation Path

3.6 Installing Authentication Provider Software

FileNet P8 platform requires that supported authentication be installed and configured. Supported authentication configurations are Windows Authentication, Sun Directory service, or Novell directory service. This paper recommends noting down the Java installation path. On our system, we installed Sun Java Directory service on SnapDrive configured local drive path. Locate the system path where the 'java.exe' program file is installed. Following figure shows the status of configuring Sun ONE directory distribution server.



```
[slapd-ibmx335-svl62]: starting up server ...
[slapd-ibmx335-svl62]: [19/Sep/2006:15:34:12 -0700] - Sun-ONE-Directory/5.2 B20
[slapd-ibmx335-svl62]: [19/Sep/2006:15:34:13 -0700] - Listening on all interfaces
[slapd-ibmx335-svl62]: [19/Sep/2006:15:34:13 -0700] - slapd started.
Your new directory server has been started.
Created new Directory Server
Start Slapd  Starting Slapd server configuration.
Success Slapd Added Directory Server information to Configuration Server.


Checking connection to the Configuration Directory Server... done.
Registering Administration Server with Configuration Directory Server... done.
Loading Administration Server tasks... done.
Loading global Administration Server configuration... done.
Generating configuration files ... done.
Writing Administration Server keys to the Windows registry... done.
Configuration of the Administration Server succeeded.
Administration server started properly.
```

Figure 13: Sun Java Directory Server Installed on Content Engine Server

4. Installation

This section discusses the procedure to install and configure FileNet P8 platform. Windows operating system and SQL Server administration expertise helps while installing FileNet P8 platform components. This paper covers information about installation tasks of content engine, process engine, application engine, and rendition engine. It also covers the postinstallation configuration tasks. This paper recommends users to refer to FileNet documentation for installing the FileNet P8 components.

4.1 Installing FileNet P8 Software

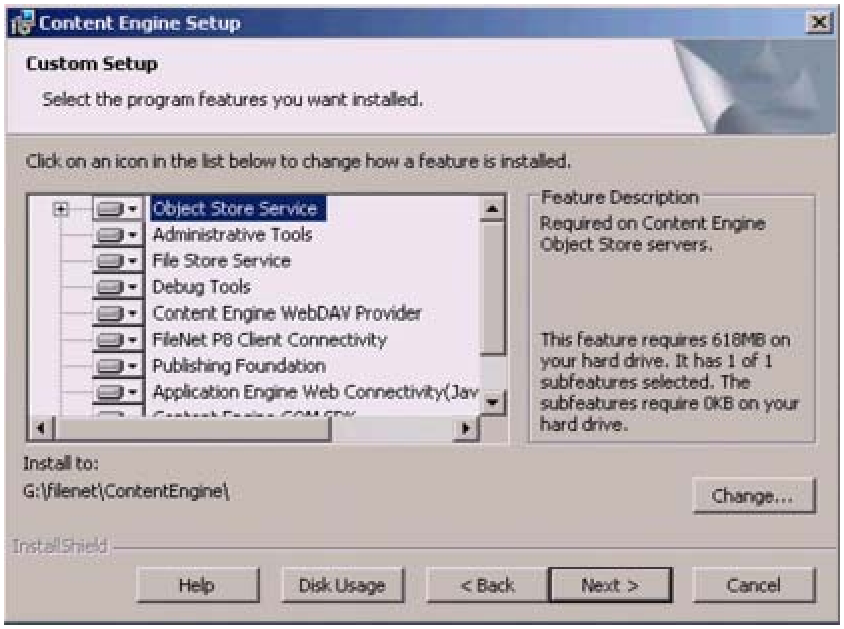
Successful installation of FileNet P8 software requires that the preinstallation tasks be completed. Section 2.2 lists the preinstallation requirements. Verify that the tasks are completed. Here is a brief checklist related to preinstallation tasks. This section describes the steps involved with installing FileNet P8 platform components. Prepare the Windows servers with appropriate Operating System and applying the required Hot Fixes. This paper describes the steps involved in our test setup in the following steps. Installing SQL Server on a dedicated server will improve performance. Installation of each component of P8 platform on a single or several machines depends on the type of configuration selected. This section lists the procedure to install the core P8 Platform components.

4.2 Installation of Content Engine Server

In our test setup, it was a fresh install of FileNet P8 Platform components. After verifying the availability of Microsoft Windows and SQL Servers, the following core FileNet P8 Platform components were installed. Upgrade the FileNet P8 components once the base installation and configurations are completed successfully. This section lists the procedure to install the content engine services. Verify the database server and authentication provider services are configured and running. Following procedure helps to understand the steps involved with the installation of content engine.

- Install the FileNet P8 Platform documentation for the application server. FileNet P8 Platform documentation includes a Java based full-text search engine; it runs as a Web-based application.
    - WebSphere or WebLogicor JBoss or Tomcat or Oracle Application Server or Sun Java Application Server
- Set up Content Engine.
    - Install Content Engine and complete the setup. Content Engine requires Windows Active Directory for authentication purposes. After installing Object Store Services, maintain the same server name. Do not rename any server once the installation is complete.
    - Create or join a FileNet P8 domain.
    - Configure the Content Engine environment by assigning permissions for the FileNet P8 Apache User and modifying the local security policy on the Content Engine servers.
    - Create an object store and verify the installation of Content Engine.
- Set up Process Engine.
- Install Application Engine.
- Set up Application Engine.
- Install Service Packs and associated Hot Fix Packs.

After selecting the content engine services to install, installation wizard prompts to enter the installation folder. In our test setup, we selected a SnapDrive created virtual local drive path G:\P8CE for setting up content engine. Select a custom setup to select the installation path and the ability to select the program feature to be installed, as shown below. On our test setup, we selected Windows Administrator’s account for WebDAV configuration.



Content Engine Setup

Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

- Object Store Service
- Administrative Tools
- File Store Service
- Debug Tools
- Content Engine WebDAV Provider
- FileNet P8 Client Connectivity
- Publishing Foundation
- Application Engine Web Connectivity(Jav

Feature Description

Required on Content Engine Object Store servers.

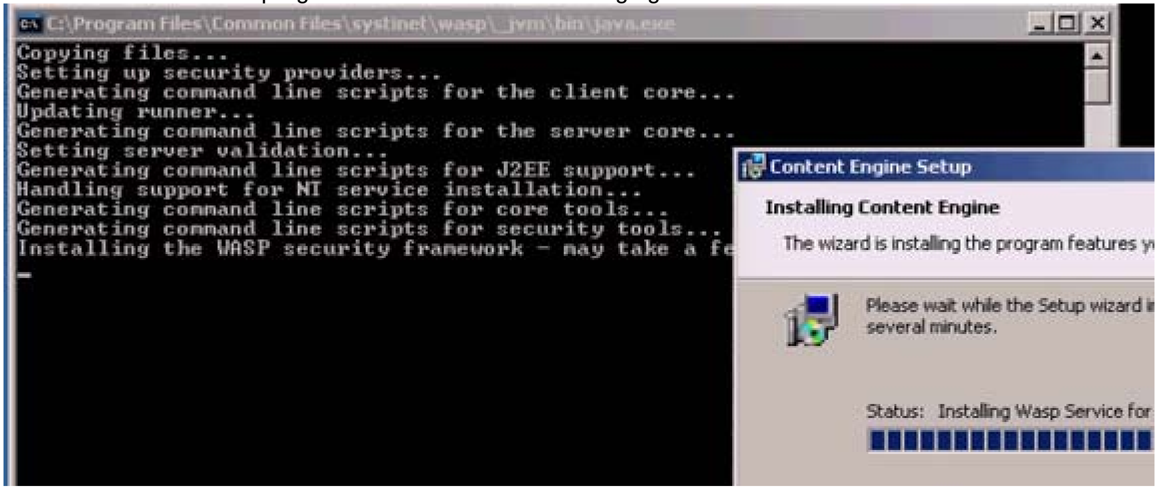
This feature requires 618MB on your hard drive. It has 1 of 1 subfeatures selected. The subfeatures require 0KB on your hard drive.

Install to:

G:\filenet\ContentEngine\

Figure 14 : Content Engine Setup – Selecting Program Features

This procedure installs and configures the Apache HTTP server application. It is important to verify the server information such as network domain, server name and the TCP port number. On our test setup, we selected the default port number 8008. If the FileNet P8 documentation is installed, provide the P8 documentation at this point. Installation utility continues with the installation after accepting the software license agreement. Following figure displays the progress of installation of content engine on our test setup. Observe the installation progress as shown in the following figure.



C:\Program Files\Common Files\systinet\wasp_jvm\bin\java.exe

```
Copying files...
Setting up security providers...
Generating command line scripts for the client core...
Updating runner...
Generating command line scripts for the server core...
Setting server validation...
Generating command line scripts for J2EE support...
Handling support for NT service installation...
Generating command line scripts for core tools...
Generating command line scripts for security tools...
Installing the WASP security framework - may take a fe
_
```

Content Engine Setup

Installing Content Engine

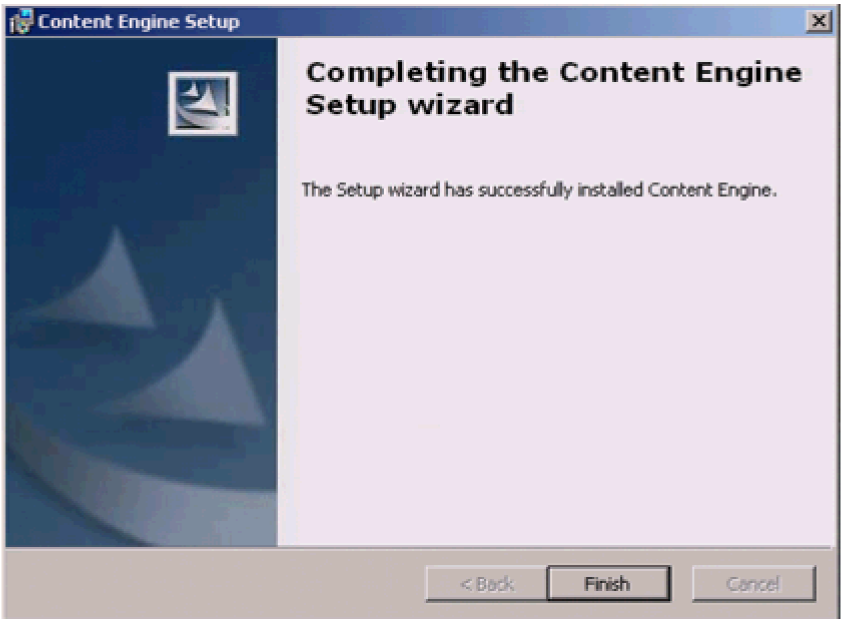
The wizard is installing the program features y

Please wait while the Setup wizard i several minutes.

Status: Installing Wasp Service for

Figure 15: Content Engine Installation Progress

After copying the necessary files, it displays the status of content engine installation as shown in the following figure.



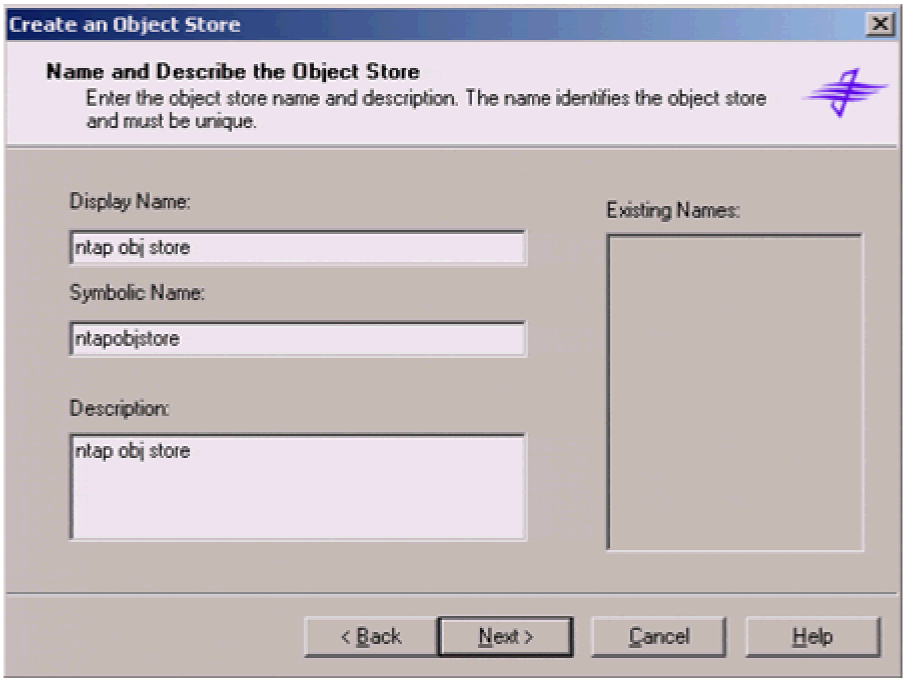
Content Engine Setup

Completing the Content Engine Setup wizard

The Setup wizard has successfully installed Content Engine.

Figure 16: Display of Content Engine Installation Status

After the installation of content engine, set up the content engine global configuration data (GCD) by selecting the user and group accounts from the directory service. This account will have the ability to create new object stores, file stores, and content cache stores. On our test setup, we proceeded to create the object store to get started with content engine. Use the FileNet Enterprise Manager to start creating the object store. On our test setup, we created the object store called ‘ntapobjstore’ as shown in the following figure.


Create an Object Store

Name and Describe the Object Store

Enter the object store name and description. The name identifies the object store and must be unique.

Display Name: ntap obj store

Symbolic Name: ntapobjstore

Description: ntap obj store

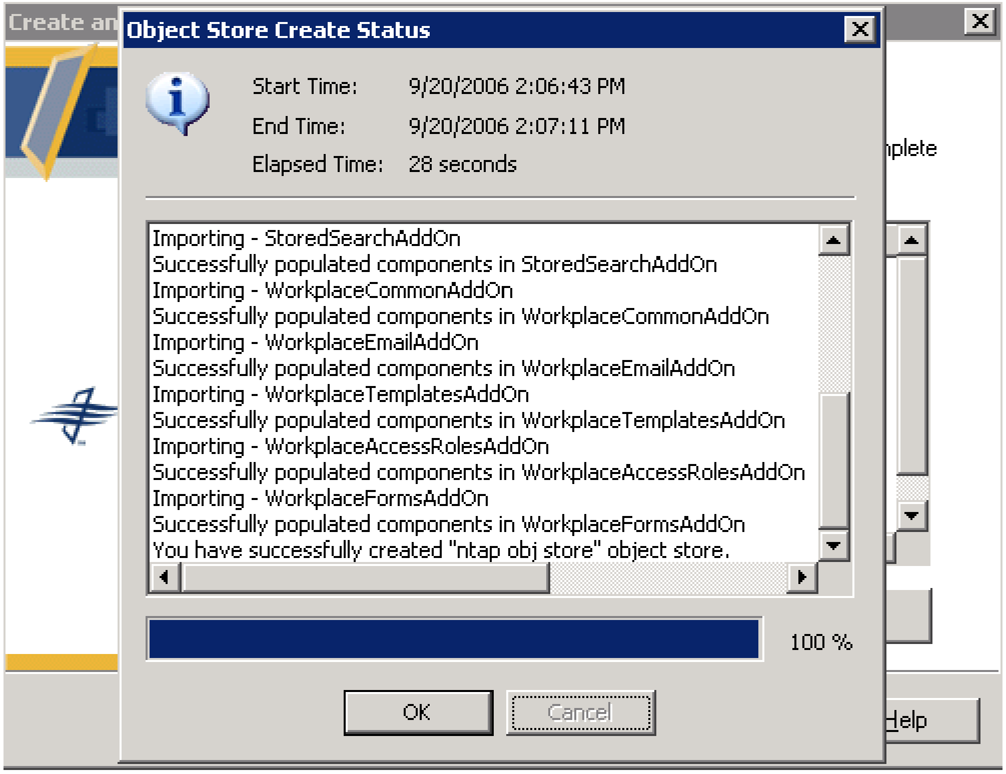
Existing Names:

Figure 17: Creating an Object Store

It is required to specify the following additional information to create an object store.

- Database server for SQL or the database alias for Oracle and DB2
- Windows account’s authentication method to specify logon information
- Choose an existing database or create a new database. Installation user must have the access permissions to complete this task.
- Default storage location for content be in the database store or in a file such as database store or file store
- Users and groups for administrative access to the object store
- Initial user groups to have basic, non-administrative access to the object store

On our test setup, we chose an existing database called CEPE8db and a SQL Server database server and selected a shared folder. On our test setup, we created a folder on SnapDrive configured drive to create a shared folder. Shared folder path also supports Universal network connectivity (UNC) path. Observe the object store create status and following figure displays a sample output from our setup.



Object Store Create Status

Start Time: 9/20/2006 2:06:43 PM
End Time: 9/20/2006 2:07:11 PM
Elapsed Time: 28 seconds

```
Importing - StoredSearchAddOn
Successfully populated components in StoredSearchAddOn
Importing - WorkplaceCommonAddOn
Successfully populated components in WorkplaceCommonAddOn
Importing - WorkplaceEmailAddOn
Successfully populated components in WorkplaceEmailAddOn
Importing - WorkplaceTemplatesAddOn
Successfully populated components in WorkplaceTemplatesAddOn
Importing - WorkplaceAccessRolesAddOn
Successfully populated components in WorkplaceAccessRolesAddOn
Importing - WorkplaceFormsAddOn
Successfully populated components in WorkplaceFormsAddOn
You have successfully created "ntap obj store" object store.
```

Figure 18: Status of Creating Object Store

After the object store is created successfully, create a new folder, new subfolder, document, or a new custom object to manage the content as shown below. Use the FileNet Enterprise Manager snap-in tool.

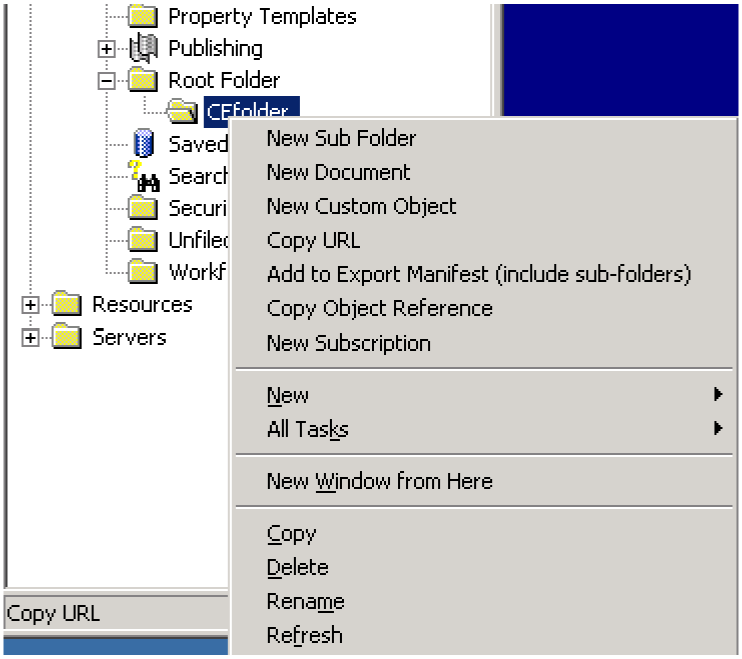
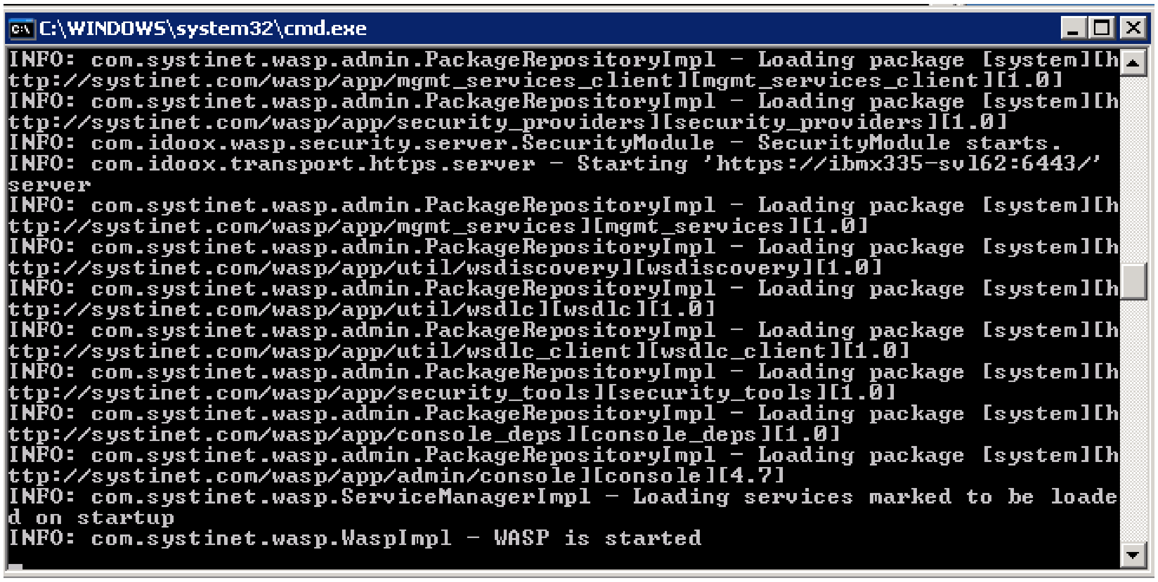


Figure 19: Creating New Subfolder, Document, or a Custom Object

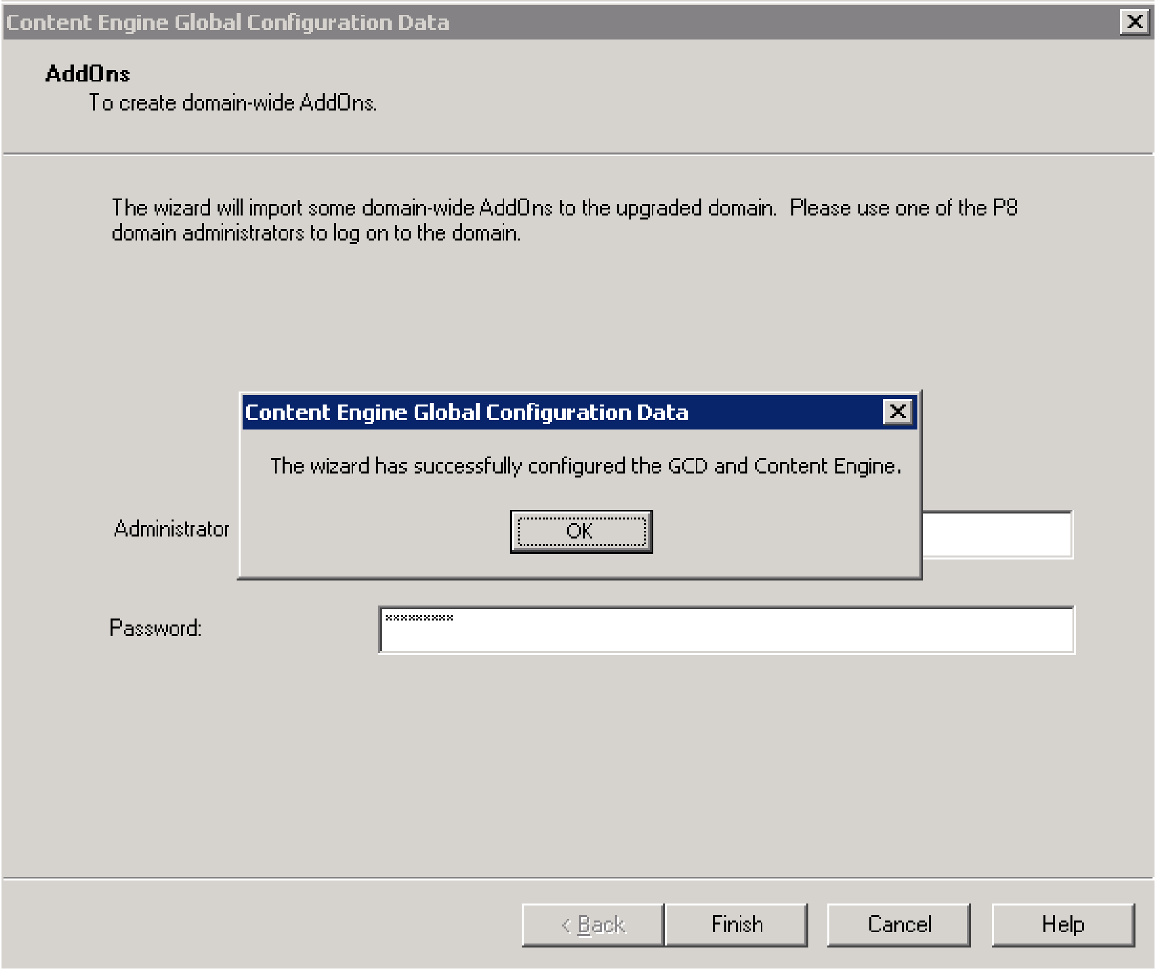
FileNet P8 content engine 3.5.2 supports SnapLock for compliance purposes. Having installed the base release, now the system is ready for FileNet P8. Now upgrade the content engine by applying the necessary service pack. Installation wizard validates the content engine install and copies the new files. Following figure displays the status of content installation before completing the upgrade process.



```
INFO: com.systinet.wasp.admin.PackageRepositoryImpl - Loading package [system][h
ttp://systinet.com/wasp/app/mgmt_services_client][mgmt_services_client][1.0]
INFO: com.systinet.wasp.admin.PackageRepositoryImpl - Loading package [system][h
ttp://systinet.com/wasp/app/security_providers][security_providers][1.0]
INFO: com.idoox.wasp.security.server.SecurityModule - SecurityModule starts.
INFO: com.idoox.transport.https.server - Starting 'https://ibmx335-sv162:6443/'
server
INFO: com.systinet.wasp.admin.PackageRepositoryImpl - Loading package [system][h
ttp://systinet.com/wasp/app/mgmt_services][mgmt_services][1.0]
INFO: com.systinet.wasp.admin.PackageRepositoryImpl - Loading package [system][h
ttp://systinet.com/wasp/app/util/wsdiscovery][wsdiscovery][1.0]
INFO: com.systinet.wasp.admin.PackageRepositoryImpl - Loading package [system][h
ttp://systinet.com/wasp/app/util/wsdlc][wsdlc][1.0]
INFO: com.systinet.wasp.admin.PackageRepositoryImpl - Loading package [system][h
ttp://systinet.com/wasp/app/util/wsdlc_client][wsdlc_client][1.0]
INFO: com.systinet.wasp.admin.PackageRepositoryImpl - Loading package [system][h
ttp://systinet.com/wasp/app/security_tools][security_tools][1.0]
INFO: com.systinet.wasp.admin.PackageRepositoryImpl - Loading package [system][h
ttp://systinet.com/wasp/app/console_deps][console_deps][1.0]
INFO: com.systinet.wasp.admin.PackageRepositoryImpl - Loading package [system][h
ttp://systinet.com/wasp/app/admin/console][console][4.7]
INFO: com.systinet.wasp.ServiceManagerImpl - Loading services marked to be loade
d on startup
INFO: com.systinet.wasp.WaspImpl - WASP is started
```

Figure 20: Content Engine Upgrade Status

Update the content engine global configuration by providing the necessary information. On our test setup, we created the content engine global configuration data (GCD) and Content Engine as shown below.



Content Engine Global Configuration Data

AddOns

To create domain-wide AddOns.

The wizard will import some domain-wide AddOns to the upgraded domain. Please use one of the P8 domain administrators to log on to the domain.

Content Engine Global Configuration Data

The wizard has successfully configured the GCD and Content Engine.

Administrator

Password: **********

Figure 21: Configuring Content Engine Global Configuration Data

4.3 Installation of Process Engine

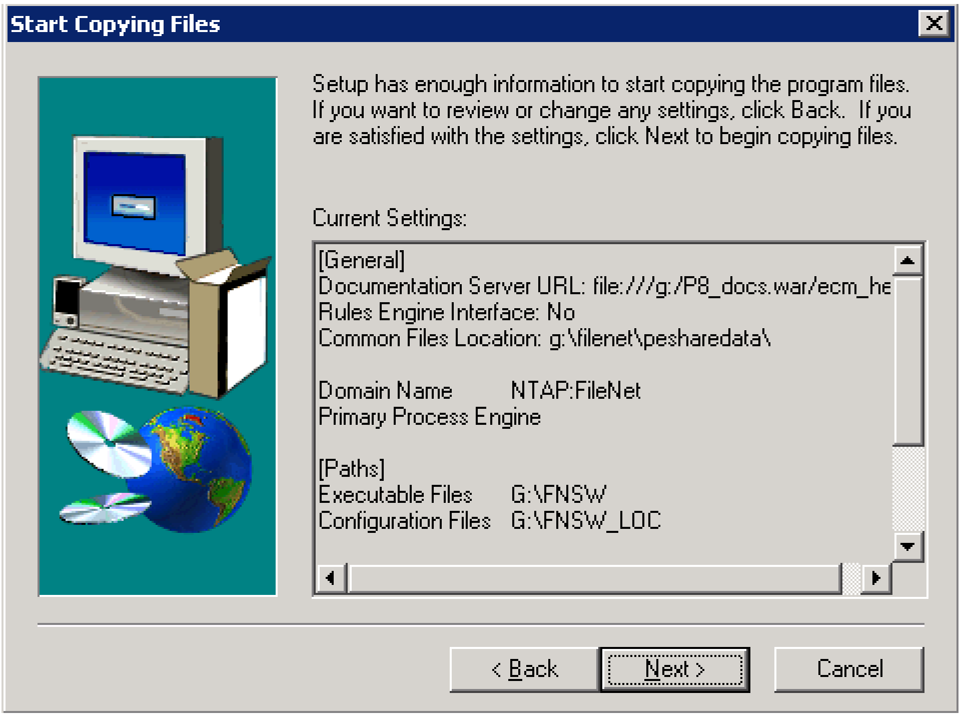
In this section, we discuss the installation of process engine services using FileNet baseline configurations. Unless it is a demonstration setup, this paper suggests installing and configuring process engine on a separate server. This section briefly discusses the procedure to install process engine on NetApp storage systems. As a prerequirement to install process engine using NetApp storage systems, verify that the necessary local drives are configured by SnapDrive and storage space is available for the application. To successfully install and configure process engine, complete the following tasks.

Verify FileNet P8 Documentation is installed and the appropriate URL is available. If not, it is possible to provide the documentation URL after the installation is over. On our test setup, we installed the P8 documentation on SnapDrive created local drive and provided the URL path as file://g:/P8_docs.war/ecm_help.

- Choose to configure rules engine or not to configure.
- Provide a location where the common configuration files will be installed for sharing with other P8 products.

- Provide the two-part Network Clearinghouse domain name. In our setup, we chose 'NTAP:FileNet' domain.
- Specify if this is primary process engine to contain the master copy of configuration database.
- Specify the location for the executable and configuration files. In our test case, we selected the SnapDrive configured drive path.
- Location of the database used as a local RDBMS or remote RDBMS. If the database instance is running on a different server than the content engine server, select the remote RDBMS option.

After providing all the information, on test setup, process engine (PE) installation wizard displayed the following output. Installation continues with the input provided and installs the process engine. By applying the appropriate service packs, complete the process of upgrading the process engine.



Start Copying Files

Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

Current Settings:

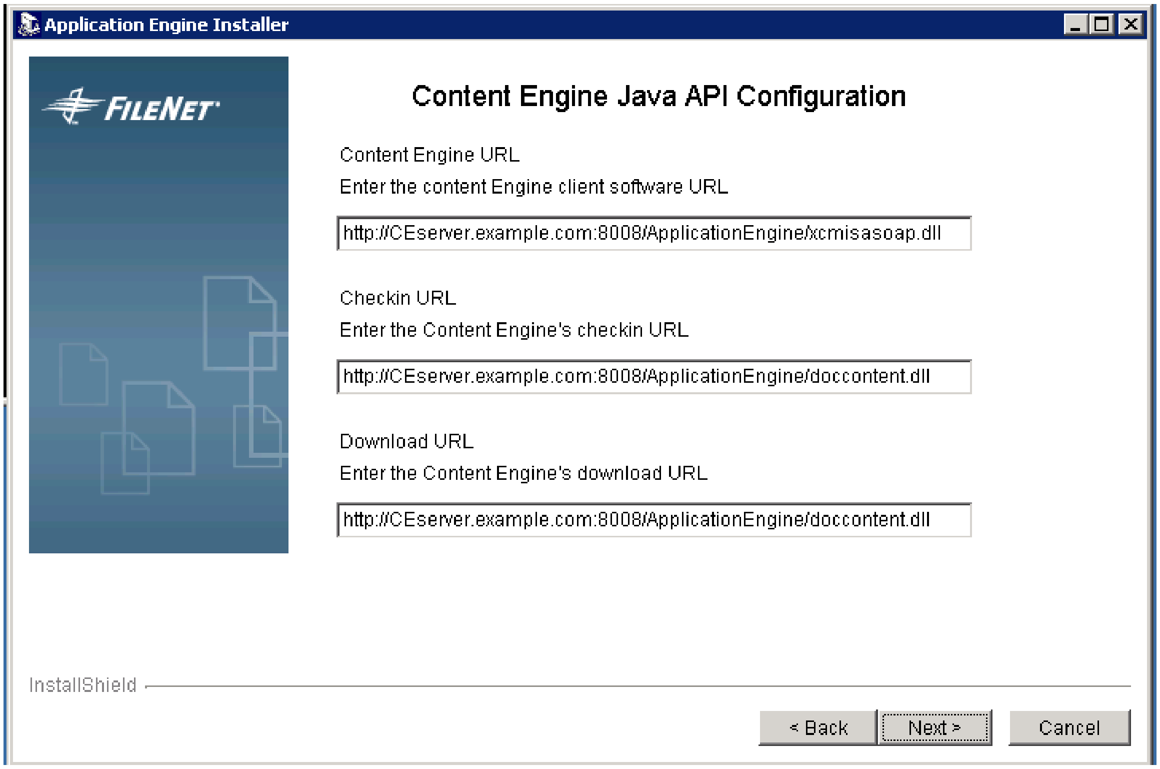
```
[General]
Documentation Server URL: file:///g:/P8_docs.war/ecm_he
Rules Engine Interface: No
Common Files Location: g:\filenet\pesharedata\

Domain Name         NTAP:FileNet
Primary Process Engine

[Paths]
Executable Files      G:\FNSW
Configuration Files   G:\FNSW_LOC
```

Figure 22: Process Engine Installation Process

4.4 Installation of Application Engine

Application Engine (AE) is the FileNet P8 component to host the workplace Web application, Java applets, process engine router and application development. Application engine protects the user credentials. In a FileNet P8 platform environment, application engine acts as a gateway to content and process to the client applications. This architecture allows the application engine to verify the user credentials before providing the access to the process and content.

In a production environment, this paper suggests installing the application engine on separate machine(s) as shown in the FileNet P8 baseline configurations in figure 1. This section provides brief information about the procedure to install application engine software. Install the storage systems and make the storage space available on the application server. On our test setup, we installed application after installing the content engine and process engine services. We selected G:\AE as the installation directory where G:\ is SnapDrive configured virtual local disk. Choose an application server configured such as Websphere, Weblogic, or Generic J2EE application server. On our setup, we selected Generic J2EE application server option. Next, provide content engine Java API configuration information. Following figure displays the URL information provided in our test setup. Installation wizard expects additional information such as user security, token security, documentation configuration. Verify that FileNet Application Engine ISRA servelet is installed successfully. This paper recommends to avoid using 'remote desktop' connection while installing Application Engine software.



Application Engine Installer

Content Engine Java API Configuration

Content Engine URL

Enter the content Engine client software URL

http://CEserver.example.com:8008/ApplicationEngine/xcmisasoap.dll

Checkin URL

Enter the Content Engine's checkin URL

http://CEserver.example.com:8008/ApplicationEngine/doccontent.dll

Download URL

Enter the Content Engine's download URL

http://CEserver.example.com:8008/ApplicationEngine/doccontent.dll

Figure 23: Application Engine Installation Information about Content Engine

4.5 Optional P8 Installation Tasks

Sections 4.1, 4.2, and 4.3 discussed the procedure to install FileNet P8 platform core components. There are several optional components available in P8 platform. Figure 11 shows the FileNet P8 platform architecture with core and optional components. This section briefly discusses the optional installation tasks available to configure FileNet P8 platform system. One can install the optional components of FileNet P8 platform in any order. Here is the list of optional components.

- FileNet Publishing components
- Process Engine Component Integrator
- FileNet Enterprise Manager on a dedicated machine
- Workplace Application Integration
- Enable Rules Engine Integration

- Web Service Integration
- FileNet System Manager
- Deploy Multiple Application Engine Instances
- Enable Application Engine to use ISRA

4.6 Creating Fixed Content Store Using SnapLock Volume

Content Engine's database is a repository of various classes and objects. Object store is a group of objects and they provide access to the client application functionality. From the end-user's perspective, object stores are presented as a list of folders or as a number of Java based Web pages. A file store is a shared folder that contains the document content on a Windows file system. FileNet P8 platform supports both NTFS file system and Distributed File System (DFS). NetApp storage system configurations of network share, IP-based SAN, or Fibre Channel based SAN setup support content store in P8 platform environment. Content store supports both NTFS and DFS file systems. This implies that NetApp VFM® (Virtual File Manager™) supports content store in both file system formats.

FileNet P8 requires a third party API to access the fixed content store. By using the NetApp SnapLock architecture, P8 exploits the NetApp open architecture. Fixed content repository is writing once while allowing the multiple reads by not allowing the content changed. Fixed content architecture enforces policy based content protection by integrating with SnapLock feature.

Enterprise data grows at a significant rate. Corporations must address the issue of data growth in addition to meeting all compliance regulations. By integrating FileNet P8 platform with NetApp storage systems, such issues are addressed effectively. NetApp storage systems provide dynamic storage scalability benefits. NetApp SnapLock offers write-once and read-many (WORM) storage and a policy based retention feature for content services. Joint solutions of NetApp storage system and FileNet P8 platform solutions exploit the advantages to meet enterprise content management challenges. Fixed content device provides the connection between the content engine and NetApp storage systems. With SnapLock and fixed content store, a document is protected from being altered or deleted until the retention period expires.

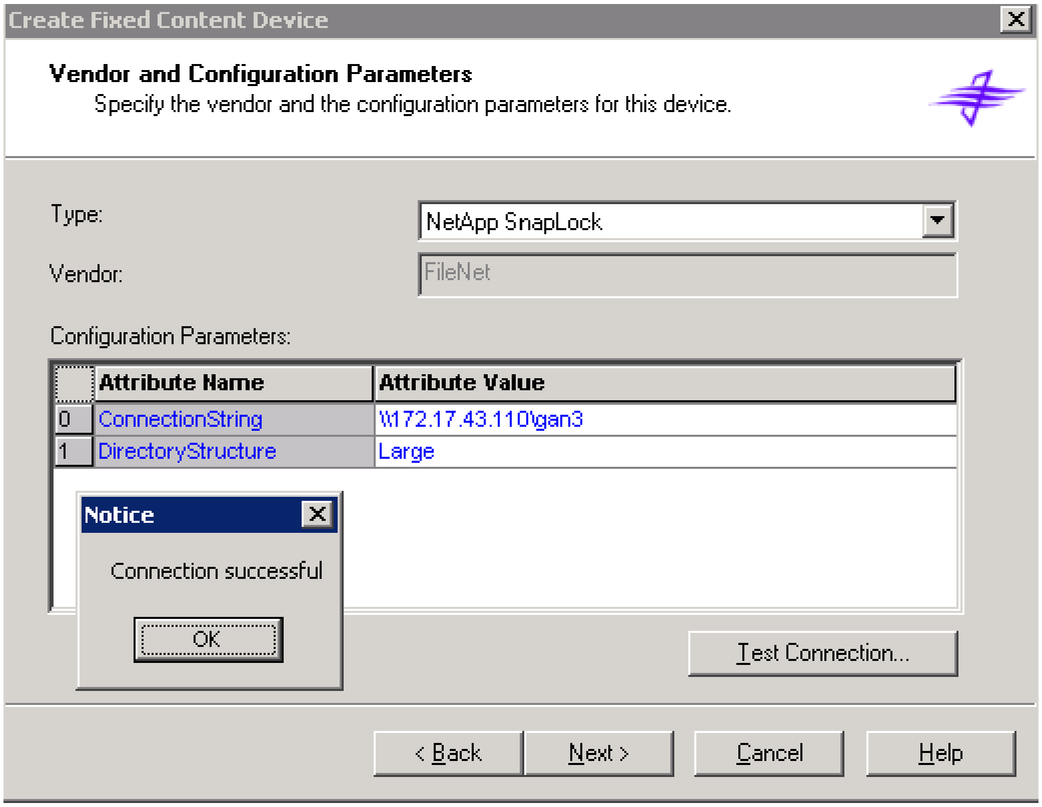
This section briefly discusses procedure to configure fixed content store using NetApp SnapLock volume configuration. To create a content engine file store on NetApp SnapLock volume, follow these steps. However, seek professional help while setting up SnapLock volume. Additional information on SnapLock is available in a technical report titled "Using SnapLock Compliance and SnapLock Enterprise with Data ONTAP 7G."

Start the FileNet P8 component services such as process engine and application engine etc. Create the necessary SnapLock volumes on NetApp storage system(s) with the appropriate configuration for the storage availability. This includes the network connectivity, creating, and configuring the SnapLock volume(s). Enable the SnapLock license(s) on NetApp storage system. Retention properties of SnapLock compliance volume on our test setup are:

snaplock_default_period=1y, snaplock_minimum_period=30d,

snaplock_maximum_period=10y, extent=off, try_first=volume_grow

Fixed content device allows managing the content in a fixed storage location by integrating NetApp SnapLock volume. Use the FileNet Enterprise Manager tool to create fixed content device. Fixed content device has a unique name within a FileNet P8 domain. Select fixed content device type as NetApp SnapLock from the available options. Following figure displays the status of SnapLock volume connectivity test on our system. If a large directory structure is required, change the directory structure attribute accordingly. Initialize the specified directory location.



Create Fixed Content Device

Vendor and Configuration Parameters

Specify the vendor and the configuration parameters for this device.

Type: NetApp SnapLock

Vendor: FileNet

Configuration Parameters:

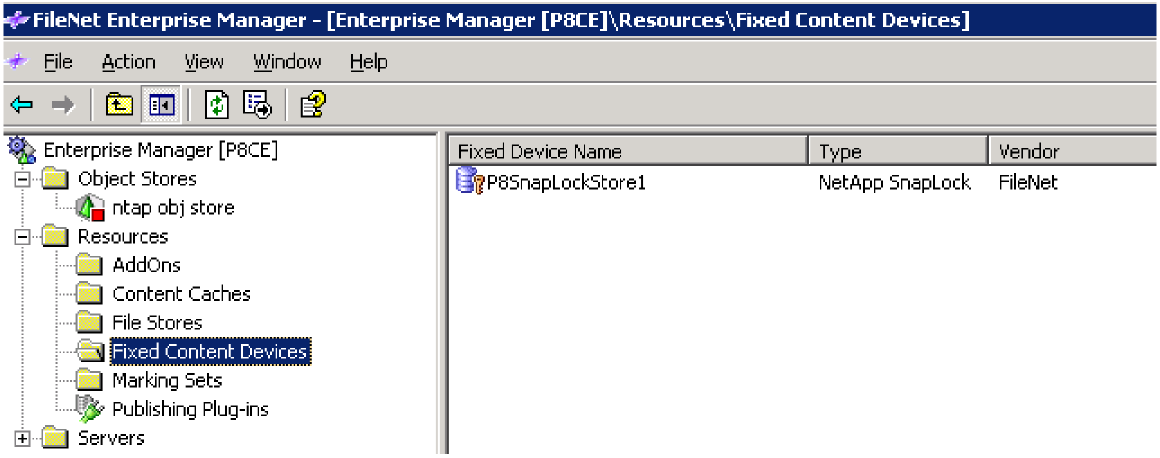
	Attribute Name	Attribute Value
0	ConnectionString	\\172.17.43.110\gan3
1	DirectoryStructure	Large

Notice

Connection successful

Figure 24: Testing Connectivity to NetApp SnapLock Destination Path

Continue with the create wizard to provide configuration information such as retention period for the content on SnapLock volume and verify the attributes of fixed content device being created to ensure the retention period. This setting includes the minimum, default and maximum retention period settings on the fixed content device. However, note that the retention period settings done on the NetApp storage system override these settings. This feature provides an additional layer of protection to ensure the retention policy of the company. This paper strongly suggests seeking professional help while configuring and testing SnapLock volume. Following figure shows the newly created fixed content device.



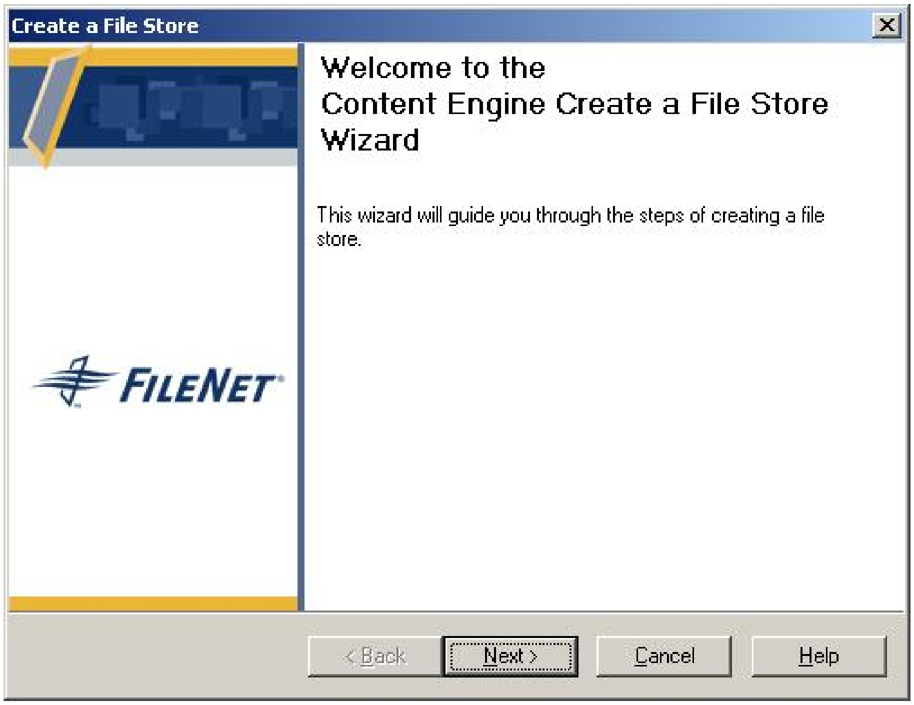
Fixed Device Name	Type	Vendor
P8SnapLockStore1	NetApp SnapLock	FileNet

Figure 25: Newly Created Fixed Content Devices Using NetApp SnapLock

Note that the retention settings on the SnapLock volume override the retention settings on the fixed device. However, it is required that the fixed device settings be exactly same as the SnapLock volume settings (user must manually enter the correct values when they create the fixed device). If these values are not accurate, the Content Engines view of the retention period may not be correct. For example, if the default of the fixed device is set to 1 month, but the actual default on the volume is 3 months, then the Content Engine will allow the *document* to be deleted after 1 month. But the underlying content cannot be deleted for another 2 months, so the file store service will have a pending delete request that it cannot apply (it will retry it every 90 seconds for the next 2 months).

This section describes how you create a SnapLock fixed device. To store content to the fixed device a hybrid file store that uses the device must be created (a hybrid file store must be created before any content can be created for a fixed device). A hybrid file store is created by running the ‘create a file store’ wizard. The user must select a file store root directory – just as they would for a normal file store. This file store is used to stage content before it is migrated to SnapLock volume and to store content that will not be migrated (content of annotations and content in the non-immutable serveration state). On the last dialog, the user selects the fixed device they want associated with this file store (making a hybrid store). If a SnapLOck device is selected, they are taken to a SnapLock specific prompts where they choose the retention period for all content stored in this hybrid file store (when it is migrated to SnapLock).

Following four figures (Figure 26 through 29) demonstrate the procedure in creating a file store. First step is to use the Content Engine’s ‘Create File Store’ wizard as shown below.



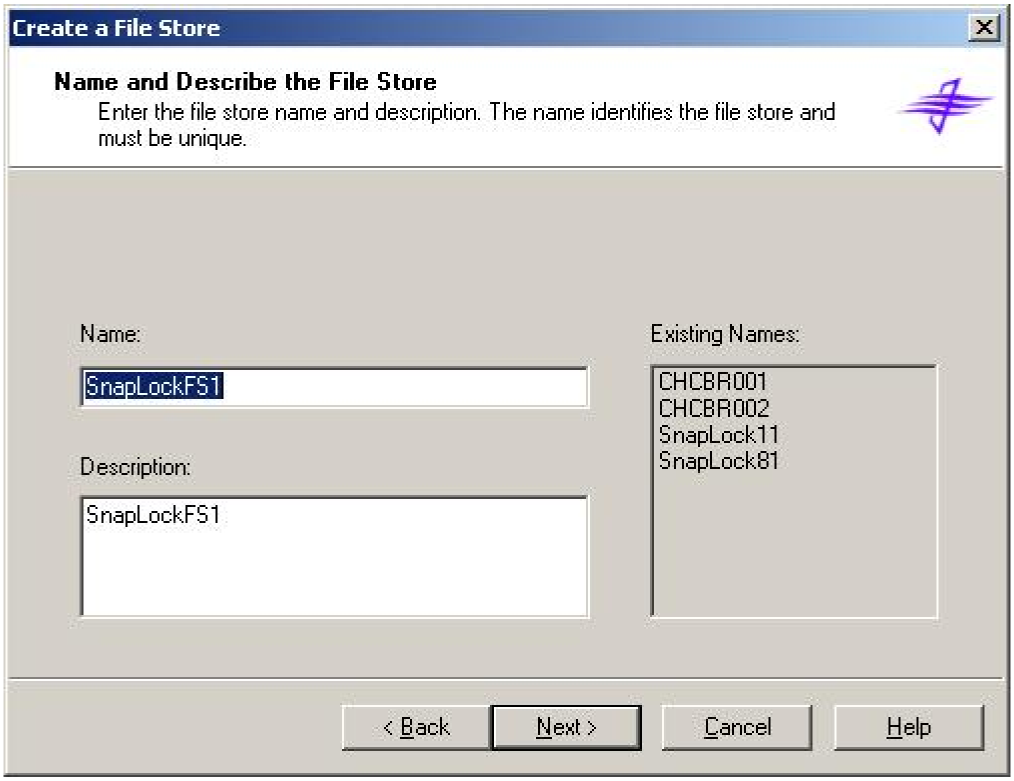
Create a File Store

Welcome to the Content Engine Create a File Store Wizard

This wizard will guide you through the steps of creating a file store.

Figure 26: Create a File Store Wizard

Enter the file store name and description to identify the file store that must be unique. In our test setup, we provided the file store name as SnapLockFS1 as shown below.



Create a File Store

Name and Describe the File Store

Enter the file store name and description. The name identifies the file store and must be unique.

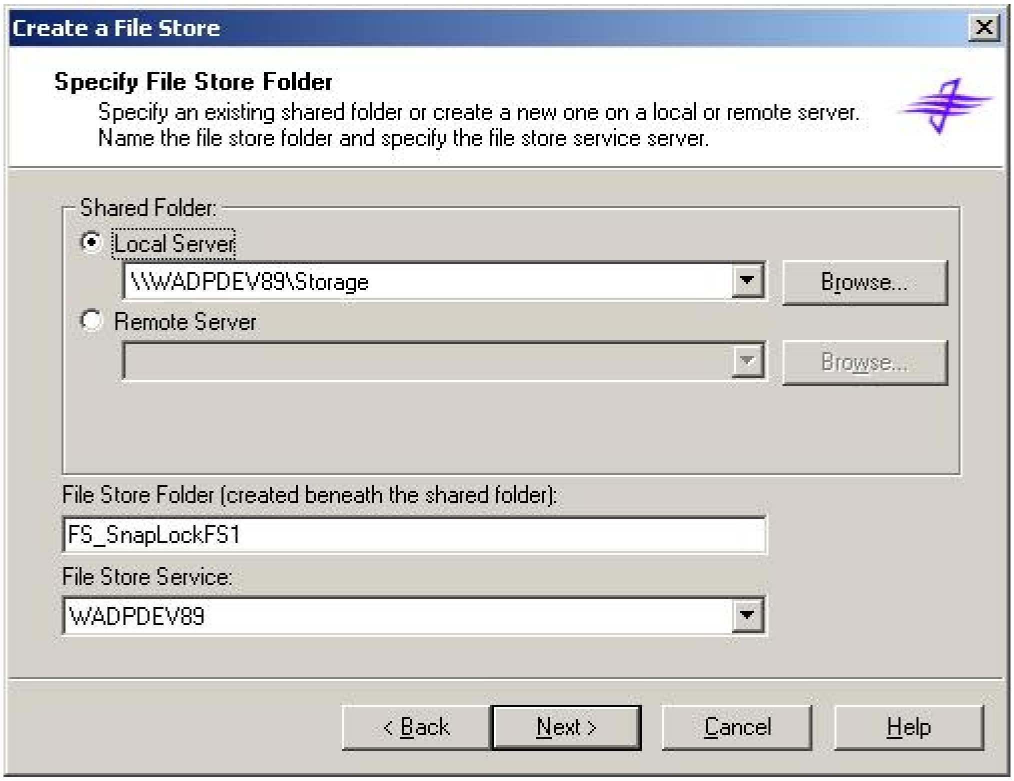
Name: SnapLockFS1

Description: SnapLockFS1

Existing Names:
CHCBR001
CHCBR002
SnapLock11
SnapLock81

Figure 27: File Store Name and Description while using Create File Store Wizard

Next step is to provide an existing shared folder or specify to create a new-shared folder. The shared folder can be on a local or a remote server. It is important to note that the file store folder will be created under the shared folder. An example is shown below.



Create a File Store

Specify File Store Folder

Specify an existing shared folder or create a new one on a local or remote server.
Name the file store folder and specify the file store service server.

Shared Folder:

● Local Server: \\WADPDEV89\Storage

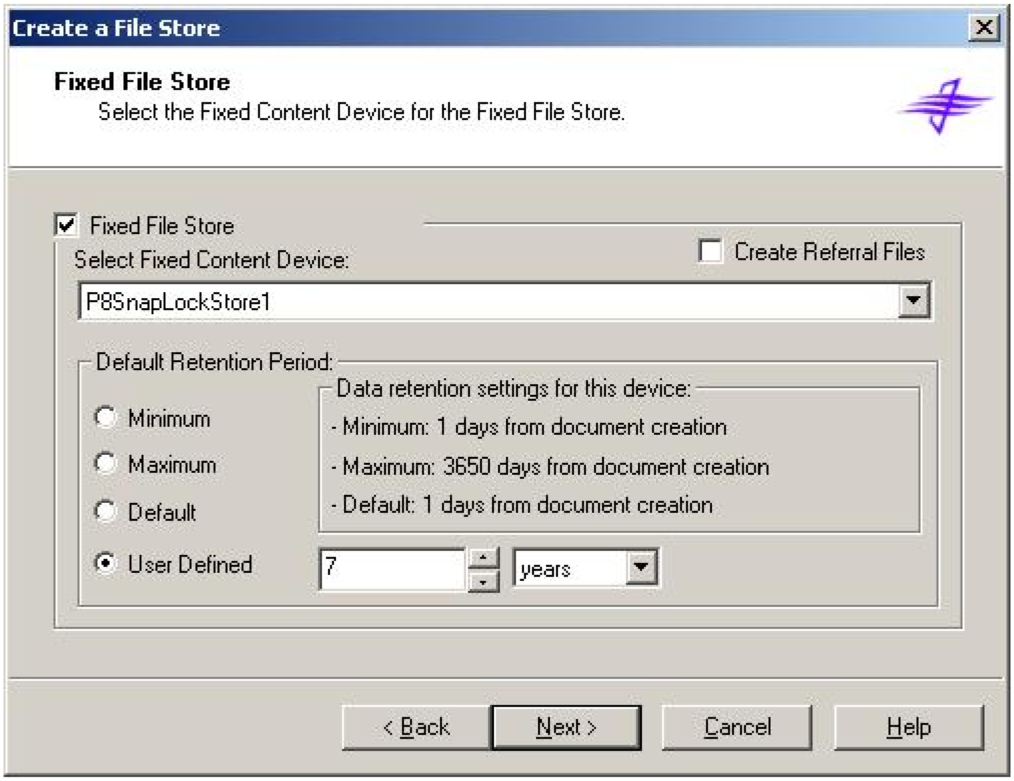
○ Remote Server:

File Store Folder (created beneath the shared folder): FS_SnapLockFS1

File Store Service: WADPDEV89

Figure 28: Specifying a File Store Folder

Next step is to select a fixed content device for the fixed content store. Best practice is to verify the SnapLock volume retention settings and specify the retention same as retention period settings on the NetApp storage system. This approach will allow the Content Server to delete the retention expired objects. In the following example, retention period was set to 7 years


Create a File Store

Fixed File Store

Select the Fixed Content Device for the Fixed File Store.

☑ Fixed File Store

Select Fixed Content Device: P8SnapLockStore1

□ Create Referral Files

Default Retention Period:

○ Minimum

○ Maximum

○ Default

● User Defined 7 years

Data retention settings for this device:

- Minimum: 1 days from document creation
- Maximum: 3650 days from document creation
- Default: 1 days from document creation

Figure 29: Select the Fixed Content Device for the Fixed File Store

4.7 Backup Using Snapshot™

Due to hardware, software and other external reasons such as user intervention, FileNet P8 platform system is prone to failure and data corruption or data loss in a production environment. This leads to a non-operational or seriously degraded P8 system. To recover from such system failure or data corruption, backup copy of data helps to recover the system or to recover from data corruption. Time taken to restore the data from backup before being able to bring the FileNet P8 system is critical in enterprise environments. By integrating the storage solutions from NetApp with FileNet P8 platform system, efficient backup and recovery options will be available. NetApp Snapshot allows almost instant backup copy of FileNet P8 using its Snapshot feature. SnapManager for SQL (SMSQL) is a NetApp provided application suite to manage the database backup and recovery for MSSQL Server. By employing this strategy, entire data of a FileNet P8 system can be restored quickly on all affected servers. This type of backup and restore configuration offers compelling enterprise-wide backup and restore solutions. For details about Snapshot and SnapRestore®, refer to Snapshot technology brochure available on our Web site. A Snapshot copy of the content services is created by using a Snapshot create syntax similar to one shown below.

snap create [-A | -V] <vol-name> <snapshot-name>

It is also important to be able to restore the data from the backup copy. Joint solution configuration of NetApp storage system and FileNet P8 platform solutions allows users to restore the data from backup copy using Snapshot and SnapRestore features. It is required to close the FileNet P8 applications before restoring the data using SnapRestore command. This approach will help to bring the FileNet P8 system services successfully. FileNet P8 data is restored by using a SnapRestore create syntax similar to the one shown below.

snap restore [-A | -V] [-f] [-t vol | file] [-s <snapshot-name>] [-r <restore-as-path>] <vol-name> |

<restore-from-path>

Today, global enterprises need to protect and quickly recover data in the event of natural or man-made disasters, operator errors, or technology and application failures. They also need an efficient way to distribute data to remote locations. Without an effective data protection and distribution strategy, operations can be brought to a standstill, resulting in loss of revenue. SnapMirror® technology mirrors data to one or more network storage appliances. It continually updates the mirrored data to keep it current and available for disaster recovery, offloading tape backup, read-only data distribution, testing on non-production storage appliances, online data migration, and more. If FileNet P8 platform is spread across different locations that need access to the same data set, access becomes a challenging task. By implementing SnapMirror, architecture FileNet P8 system can be effectively replicated between sites and enables users to bring the system quickly to a disaster location. For details on SnapMirror, refer to SnapMirror best practices technical report.

5. Summary

Corporate customers are in need of robust ECM solutions that integrate easily with their existing information systems. FileNet provides solutions to manage the content generated throughout the organization. It is important to provide access to the content generated to those who need it immediately. FileNet P8 architecture provides enterprise-level scalability to address the challenges of enterprise content management. FileNet P8 architecture enhances the content and process management across an enterprise.

FileNet P8 platform customers are required to plan for an efficient backup and recovery strategy. In addition to backup and recovery, they need to plan for high data availability along with the ability to address huge data growth. Corporate regulations have forced companies to protect the content generated within the organization. These are some of the challenges encountered by FileNet P8 platform customers. Backing up of SQL, databases could take a significant amount of time and resources. An effective database backup and recovery strategy is also required. Data replication could take a significant amount of time and resources.

NetApp storage solutions effectively address the shortcomings explained previously. FileNet P8 platform and NetApp product joint solutions offer highly available and exceptional performance at a lower total cost of ownership in the industry.

NetApp and FileNet are committed to provide FileNet P8 platform users with improved solutions designed to meet their business objectives. NetApp storage system solutions ensure protection of FileNet P8 platform data and keep it highly available.

NetApp offers complete solution for FileNet P8 platform. SnapManager for SQL (SMSQL) allows a transparent method for consistent and quick backup copy of SQL database. SMSQL also allows restoring the database backup from Snapshot created. SnapDrive for Windows provides an efficient and easy way of data storage management on Windows server. SnapManager for Exchange is ideal to manage Exchange server data management such as backup and recovery.

In conclusion, the recommendations made in this paper are intended to be an overview of best practices for most environments. This document applies to version 3.5.x of FileNet P8 product. and serves as a starting guide when designing and deploying FileNet P8 Platform in a NetApp storage system(s) environment. To ensure a supported and stable environment, become familiar with the configuration and setup plans.

6. Caveat

NetApp has not tested all possible combinations of hardware, storage architecture and software solutions. If you use a different Windows Server OS or a different version of FileNet software, then significant differences in your configurations could exist. These differences could alter the procedures necessary to achieve the objectives outlined in this document. If you find that any of these procedures do not work or find any errors, we suggest contacting the author immediately. If you need additional information or have any questions, contact the Web administrator of Network Appliance, Inc. Do not attempt to seek help from NetApp Global Support team for the content accuracy or the procedure listed in this document.

7. Appendix

This section provides additional information that helps successful installation and configuration of FileNet P8 Platform components on Windows server.

7.1 Operating System Required Patches

The section lists the required hot fixes installed before configuring the NetApp Storage system using Fibre Channel Protocol and SnapDrive software. Microsoft support team provides these patches directly to its customers.

If you installing and configuring local drives using SnapDrive in Fibre Channel Protocol environment, following Windows hot fixes are required on Windows 2003 SP1 server.

1. Q916531-hbaapi
2. Q916048-storport
3. Q913648-vss
4. Q912593-classpnp
5. Q910048-ntoskrnl

7.2 Preinstallation Checklist

Before proceeding further, complete Operating System requirements including the storage requirements. Complete the preinstallation tasks as discussed in Section 2.2.

- Windows Server 2003 Standard Edition or Enterprise Edition
- Windows 2000 Server, Advanced Server and Datacenter server
- Windows Domain Configuration
- P8 Platform Authentication such as Microsoft Active Directory
- Create P8 platform users and groups
- Installation of Windows Server, Necessary Service Pack
- Install database server, server for CE and PE
- Recommended Windows HotFixes listed in Appendix-A
- On Windows platform, boot partition must be NTFS
- Windows Domain Controller must have a static IP address
- Windows domain must have the DNS Server component installed and configured

- Set up and Configure domain controller
- Network settings such as TCP/IP, DNS
- Verify DNS configuration settings
- Configure for Windows Authentication, Sun Java System Directory Server, or Novell eDirectory

Additionally, on Windows platform, following information is referred to as optional information.

- Outlook 2003 and CDO Components, if Email Content to be managed in Outlook environment
- SQL Server 2000
- Optional Available Exchange Server 2000 or 2003
- Exchange System Manager, if Exchange Server installed in P8 Platform architecture
- P8 Platform Authentication such as Microsoft Active Directory
- MSXML - If not already installed
- MDAC – If not already installed
- .NET Framework – If not already installed
- COM+ Configure and Enabled
- MSDTC Configured and Enabled
- IIS with Active Server Pages – Include SMTP, NNTP services
- MSMQ - If not already installed

7.3 References

Following technical reports and system manuals were referenced while developing this paper. For detailed procedure, read the appropriate product documents.

1. "Integrating FileNet Image Services with NetApp Unified Storage For Windows Platform"
2. "FileNet P8 Platform Installation Guide"
3. "FileNet P8 System Overview"
4. "Integrating FileNet Image Services Connector for SnapLock with NetApp Storage"
5. "WORM Storage on Magnetic Disks Using SnapLock Compliance and SnapLock Enterprise"
6. "Multiprotocol Data Access: NFS, CIFS, and HTTP"
7. "Simple Disaster Recovery of FileNet On Windows: Image Services Using SnapMirror Technology"