EMC Centera Compliance Models Governance Edition and Compliance Edition Plus

A Detailed Review

Abstract

This white paper describes features supported by EMC® Centera® Governance Edition (GE) and Compliance Edition Plus (CE+) in order to assist in a comprehensive understanding of these products' capabilities.

June 2008

Part Number H4497

Table of Contents

Executive summary

An environment that is becoming increasingly subject to external and internal regulations and supervision adds an extra challenge onto today's organizations, which are determined to provide their customers with exceptional service and a satisfying experience. The scope and number of requirements and regulations facing businesses today are increasing – along with the costs of ensuring they are complied with.

Even though the cost of compliance can be considerable, the legal and goodwill risks associated with noncompliance can be even higher. Compliance initiatives in all business areas are increasing and often require more than simply archiving the data. Advanced technologies offer the opportunity to improve compliance results and minimize potential risks, while lowering the overall cost of compliance management.

EMC® Centera® is a simple, affordable, power-efficient and secure repository purpose built for information archiving to keep static and infrequently changing digital information available online for immediate access. EMC Centera enhances business value by capturing and preserving original content and ensuring complete, reliable integrity for the life of the archived information.

Supported by unmatched retention and disposition management capabilities EMC Centera successfully addresses the most rigorous compliance regulations, while minimizing the total cost of ownership. EMC Centera enforces organizational and application policies for information retention and disposition intrinsic in storage—and by doing so completes the information chain of custody. It ensures corporate accountability and reduces the costs of legal discovery and litigation support—and it's easy to manage.

Introduction

This white paper presents detailed information regarding the compliance options and features offered by EMC Centera, the differences between the Governance Edition and Compliance Edition Plus models, as well as a comprehensive view of the more advanced retention management capabilities: Event Based Retention, Litigation Hold, and Min/Max Governor. Finally, it provides a summary of the remote management options available per model, and references to sources of additional information.

Audience

The intended audience is customers, including storage architects and administrators and any others involved in evaluating, acquiring, managing, or designing an EMC archiving environment. This includes EMC staff and partners for guidance and development of proposals. This paper is not intended to provide guidance to software vendors on how to implement EMC Centera Compliance features, or to replace the standard EMC Centera documentation.

Terminology

- Access Profile: Access profiles are used by applications and users of management tools to authenticate to a cluster, and by clusters to authenticate to another cluster for replication or restore connections. System administrators can create access profiles using the CLI. Each access profile consists of a profile name, a secret (password), and a set of capabilities and roles.
- Centera API / Centera SDK: The EMC Centera SDK is a set of cross-platform application programming interfaces (API) that make it simple for customer applications to perform functions such as store, retrieve, delete, and query for data objects in a variety of flexible and powerful ways. All applications must use this API to read and write to EMC Centera.
- Centera Capabilities: Pool-bound content access rights granted by the system administrator to an access profile. They determine which operations an application can perform on the pool data. Possible capabilities are write (w), read (r), delete (d), exist (e), privileged delete (D), query (q), clip copy (c), Purge (p), and Litigation hold (h).
- Centera CLI: The EMC Centera Command Line Interface (CLI) is a tool for system administrators to manage and monitor EMC Centera.
- Centera Cluster: A cluster is a single logical CAS archive that is accessible to an SDK-based client application. Client applications can store, retrieve, and delete fixed content objects from a cluster. A single cluster can be accessed by one or more applications via a set of node IP addresses and access profiles. Clustered nodes are automatically aware of nodes that attach to and detach from the cluster.
- Centera Pool: *Note: In the context of this document, Centera Pools refer to Virtual Application pools.* A virtual pool (VP) is a logical construct that effectively subsets the cluster, allowing controlled data segregation with the granularity in access protection it implies, simple management, and capacity reporting capabilities.
- CentraStar®: EMC firmware used by EMC Centera
- Cluster Mask: Defines the server EMC Centera capabilities that access profiles can enable. At the cluster level, the cluster (authorization) mask is used to override other profiles.
- Content Address: A data object's unique identifier. A Content Address is the claim ticket that is returned to the client application when an object is stored to the archive.
- Content Address Storage (CAS): An object-oriented, location-independent approach for archiving large quantities of fixed content data.
- Node: Logically, a network entity that is uniquely identified through a system ID, IP address, and port. Physically, a node is a computer system that is part of the EMC Centera cluster.
- Node Role: The roles that can be assigned to each individual node are either external or internal. Nodes with an external node role have an external IP address configured and use their Eth2 port for

communication with the customer's network; external roles are access¸ management, and replication. Storage role is the only internal role. Refer to the online help for additional information.

- Pool Mask: Defines the EMC Centera capabilities granted to a particular virtual pool.

EMC Centera compliance models

EMC Centera offers three compliance models or editions: Basic, Governance Edition (GE), and Compliance Edition Plus (CE+). EMC Centera relies solely on the application to perform any disposition actions, as data will not be deleted automatically, and depending on the compliance model, it will prevent the deletion of data still under retention.

Basic model

In its Basic edition, EMC Centera delivers the full power of content addressed storage (CAS). Self-configuring, self-managing, and self-healing, it captures and preserves original content, protecting the context and structure of electronic records. However, data retention is not enforced and advanced features such as shredding and advanced retention management are not available. Data can be deleted at any time, provided the application has the appropriate access rights, regardless of the retention period initially set.

Governance Edition (GE) model

Governance Edition provides the retention capabilities required by organizations to responsibly manage electronic records, on top of the features provided by EMC Centera Basic. Deploying Governance Edition enforces organizational and application policies for information retention and disposition. You can capture and preserve original content—and ensure complete, reliable integrity for the life of your archived information.

Compliance Edition Plus (CE+) model

Compliance Edition Plus exploits the core strengths of the EMC Centera platform while adding extensive compliance capabilities to the Governance Edition model. CE+ is designed to meet the requirements of the most stringent of regulated business environments for electronic storage media as established by regulations from the U.S. Securities and Exchange Commission (SEC), the Australian AS 3806 Compliance Programs, or other national and international regulatory groups.

In Compliance Edition Plus, the system administrator can only connect to a node that has the management and/or storage role. If there is no node with the management role you need to connect directly to the Eth2 port of a node with the storage role and assign the management role to a node with no other external node role.

EMC Centera compliance features

EMC Centera offers a very comprehensive set of compliance features. Table 1 lists the features supported by each of the three models. Detailed information on each feature is presented in the following sections.

Table 1. EMC Centera compliance features by model

Feature	Basic	Governance Edition	Compliance Edition Plus
Enforces Retention	No	Yes	Yes
Retention Classes	No	Yes, Classes may be shortened or lengthened	Yes, Classes may only be lengthened
Audited Delete	Yes	Yes	Yes
Privileged Delete	Yes	Yes	No
Default Retention Period per Pool	No	Defaults to Zero	Defaults to Infinite
Configurable Default retention period per pool	No	Yes (defaults from Zero to infinite)	No
Data Shredding	No	Yes	Yes
Remote Management	Yes	Yes	No
Min/Max Governor	No	Yes (requires Advance Retention Management)	Yes (requires Advance Retention Management)
Event Based Retention (EBR)	No	Yes (requires Advance Retention Management)	Yes (requires Advance Retention Management)
Litigation Hold (LH)	No	Yes (requires Advance Retention Management)	Yes (requires Advance Retention Management)

Notes

A GE or CE+ model cannot be configured to a less stringent model.

Raw read will not receive any Event Based Retention or Litigation Hold events or information. Replication is the only supported data recovery mechanism for compliant data

Retention overview

Each data object stored on an EMC Centera can have a retention period assigned that enables organizations to impose policies around records retention. The retention period is the length of time that a data object must be retained before an application is allowed to delete it on a compliant EMC Centera. A GE or CE+ cluster will take the retention policy as passed down by the application as it stores content and enforce the policy at the individual object level, guaranteeing that the records cannot be deleted prior to the expiration of the defined retention period.

A content object stored in EMC Centera has two components:

- The unique content object, referred as a **BLOB**
- An associated Content Descriptor File (**CDF**) that is inextricably linked to the stored content

The CDF contains both a write date/time stamp and the retention period for that content. If the application makes any attempt to delete that content before the retention period specified in the CDF has expired, EMC Centera will deny the delete request. Since the only method of deleting content is through the controlling application, EMC Centera securely retains content for the duration originally specified by the application.

EMC Centera offers an application the ability to manage the retention of each content object individually, through its CDF, rather than at the tape cartridge or optical platter level (each of which may contain tens of thousands of records each). The ability of EMC Centera to automatically enforce the stated retention period contained in the CDF provides a systematic and complete method for managing the disposition of each electronic record. This is not possible using tape or optical media, which do not allow independent management of stored records.

Retention periods are set and enforced at the CDF level, not at the BLOB level. If one content object is stored by multiple applications or in multiple application contexts, the Content Addressing of EMC Centera will guarantee that the content is only stored once (also known as Single Instancing Storage). However, each storage instance will generate unique metadata and potentially a different retention period. This means that two CDFs pointing to the same BLOB may set different retention periods. While the individual CDFs can be deleted when their retention period expires, the underlying BLOB will only be removed if all CDFs that point to it are removed (that is, the longest retention period is enforced).

CDF creation dates are based on the EMC Centera cluster time, not on the clock of the application server. This reliance on cluster time guarantees that retention periods for a single CDF will expire as expected independent from application server time, different time zones, and local time changes.

The following hierarchical retention period setting applies to each data object stored on EMC Centera:

- **Application setting**: The application can assign a fixed retention period or a retention class to the CDF during its creation. The application setting of the retention period overrules the pool and cluster retention setting. Note that a CDF can only be deleted if the retention class to which it is assigned is defined on the cluster.
- **Pool setting**: If a CDF does not have a retention period or class assigned by the application, the *default retention period of the pool* applies to the CDF. The pool setting of the retention period overrules the cluster retention setting.
- **Cluster setting**: If the CDF does not have a retention period or class assigned by the application and if the pool has no default retention period, *the default retention period of the cluster* applies to the CDF.

It is the role of the application to set the retention periods that EMC Centera enforces, and to store, retrieve, and dispose of content as required. Once the retention period of a content object has expired, the application must dispose of the content by way of the Centera API; normal delete operations will fail on GE and CE+ models when attempting to dispose objects still under retention. A cluster will never proactively dispose of content managed by an application.

Note: The data will not be deleted automatically. It is the responsibility of the application or end user to delete it.

Retention periods

A retention period provides a simple mechanism for defining retention periods for CDFs. However, once you write a CDF with a retention period, you cannot change the retention period for that CDF.

Note: The retention period is calculated from the date that the CDF was created (the creation date) and not from the last modification date. If you open a CDF and write a new copy, both CDFs will have the same creation date. The retention period of the second CDF will be based on the creation date and not on the modification date.

Retention classes

Retention classes provide a way to manage and change retention periods for a set of data objects. Contrary to fixed retention periods given by the application or the pool, the retention periods assigned to a retention class can be changed by the system administrator. A retention class exists as a symbolic representation of a retention period. You associate the retention class name—not the period itself—with a CDF. A retention class acts as a retention policy that governs all CDFs cluster-wide for those CDFs assigned to that retention class. If you change the time period of a retention class, it likewise affects the retention period of all CDFs referring to that class, without changing the individual CDFs. You can define up to 1,000 retention classes in EMC Centera, which can be defined only via the CLI. The SDK allows the setting up and removal of retention class assignments on CDFs.

For example, a company with an email archiving policy of one year might define a retention class called EmailArchive with a retention period of one year. All emails are then stored on the EMC Centera with the EmailArchive retention class. If the company later changes its email archiving policy, just the EmailArchive retention class can easily be modified, effectively changing the retention period for all email content on the EMC Centera cluster.

Note: When specifying a retention class using the CLI, the time entered is translated into seconds. This translation assumes 30 days in a month and 365 days in a year.

Default retention

Default retention periods are applied to content archived in EMC Centera whenever the application does not specify a retention period or class.

Default retentions are specified either at the application pool level or at the cluster level.

Notes:

A retention policy of 0 is considered a valid policy.

Legacy CDFs with no retention information will also verify the default retention period for its pool when a delete request is received.

Default retention on Governance Edition clusters

- New pools will have the default retention period set to zero (0).
- The default retention period is defined per pool, enabling different default retention periods by application; use the `update pool retention` CLI command.
- The SDK will set the C-Clip retention period in the CDF to the pool default retention if no retention policy is specified by the application.
- When creating a CDF under EBR, and the application does not specify a fixed retention policy, a 0 retention period is added instead of using the default retention.
- The default retention period can be shortened or extended; changing the default retention period does not impact existing CDFs, only CDFs written from that moment on

Note: The new pool settings will only be effective after reconnecting the application to the EMC Centera cluster.

Default retention must be within the Min/Max settings – if not, a warning is issued. See more details in the “Min/Max Governor“ section of this document.

Default retention on Compliance Edition Plus clusters

- The default retention period is defined at the cluster level and is fixed:
  - Infinite for non-EBR CDFs
  - 0 for fixed retention period for EBR CDFs
- When upgrading to CE+, the existing Default Values are set to infinite and are no longer changeable.

Note: The default retention period prompt in the CLI `update pool retention` *command does not appear on CE+ models.*

Audited Delete

EMC Centera provides a full audit trail of each CDF that is deleted. When the SDK issues a delete call, the CDF is removed and a reflection is created. The reflection does not contain any application data or metadata but contains:

- A trace of the create and delete time
- The retention policy or policies provided
- The access profiles that executed these actions
- A Reason String, if provided by the application

The audit information can be retrieved by an application using the Query functionality. For more information refer to the *EMC Centera SDK API Reference Guide*.

Note: Audited Delete is available in Basic, GE, and CE+ modes.

Privileged Delete

Privileged Delete is an option when using Audited Delete that allows enterprises to comply with strict European Union and U.S. privacy laws. With Privileged Delete, applications can initiate a highly controlled and audited removal of information that is still under retention, including CDFs that are under Event Based Retention.

Notes: Privileged Delete is only available in GE mode. CDFs that are under Litigation Hold cannot be deleted.

EMC Centera Data Shredding

While maintaining the long-term integrity of stored content is of critical importance to any organization, it is equally important for that organization to dispose of content that is no longer of value, or is no longer required to be retained. For every compliance officer who seeks to preserve content for a specified duration, there is a colleague in the Legal department who seeks to eradicate that content as soon as it is practicable. Organizations actively seek to avoid situations where files are not properly disposed of and unwanted files are recovered or re-created in the course of litigation.

When an application deletes a CDF, all files referenced by that CDF are processed by an EMC Centera process called Garbage Collection that will delete the file if no other CDFs are still referencing that file. To ensure that deleted content is not recoverable by any means, including sophisticated microscopic disk scanning techniques, CentraStar adds an optional Data Deletion Enhancement feature. This feature is more popularly referred to as data shredding.

Organizations that must conform to security standards such as those prescribed by the U.S. Department of Defense (DoD) are required to ensure that data deleted through their applications cannot be recovered. The DoD 5015.2 standard describes the method for safely deleting content from the storage device used by the application to manage content.

The EMC Centera shredder uses the DoD 5015.2 recommended seven pass overwrite pattern. An EMC Centera with shredding enabled will move all deleted content immediately to a shredder bin outside the access path for processing by the shredding service. The shredder service will periodically (every 15 minutes) shred the content found in the shredding bin to be completely obliterated from the system.

The shredding process is autonomous from the user application. Accessing, disabling, or interfering with the shredder service is not possible by the system administrator or the application. This is part of the EMC Centera security measures to ensure that content cannot be altered, deleted, or accessed via an unauthorized user.

Note: Shredding is an exceptionally disk-intensive activity that increases the wear of the disks; for each Garbage Collection delete there are seven shredding deletes imposed to the disks. Therefore EMC recommends to only enabling shredding if required by regulations.

Advance Retention Management

A separate license enables the advanced management of data retention. This Advanced Retention Management (ARM) license enables three features: Event Based Retention, Litigation Hold, and Min/Max Governor. EMC Service personnel will install this feature, available only on GE and CE+ models, when an ARM license is purchased.

Note: ARM is licensed per four- node increments using EMC Centera model number CNR4NADVRMLIC.

Event Based Retention (EBR)

The United States Department of Defense (DoD) defines Event Based Retention (EBR) as a "disposition instruction specifying that a record shall be disposed of a fixed period of time after a predictable or specified event"; it allows applications to specify a retention policy that only starts at the time of such an event, some undetermined period of time after the CDF was created. When a CDF is marked for EBR, it cannot be deleted prior to the event unless a Privileged Delete on a GE model is used.

When using EBR, the CDF life cycle is as follows:

1. **Create**: The application creates a new CDF and marks it as being under EBR. The application can provide a regular retention period that acts as a sort of minimum retention and must provide an Event Based Retention policy in the form of a period or class.

2. **Trigger Event**: The application triggers the event, which in essence starts the clock on the Event Based Retention policy. At this point the application can provide a new Event Based Retention policy, provided it is longer than the one provided at the time of the CDF create.

3. **Delete**: When the application tries to delete the CDF, the following conditions must be satisfied:
   - Fixed retention has expired.
   - The event has been triggered.
   - Both the Event Based Retention set at the time of creation and (optionally) the one set at the time of the event have expired.

Notes: Retention Period or Class must comply with rules for Default Retention and Min/Max Governor.

Privileged Delete can override both fixed and variable retention policies.

Applications that use the EBR feature must have the (w) capability enabled and use SDK 3.1 or later.

Figure 1 shows the three possible scenarios for a CDF being put under Event Based Retention:

• C1 has a fixed or minimal retention that already expired before the event was triggered.

• C2 has a fixed or minimal retention that will expire before the EBR expires.

• C3 has a fixed or minimal retention that will expire after the EBR expires.

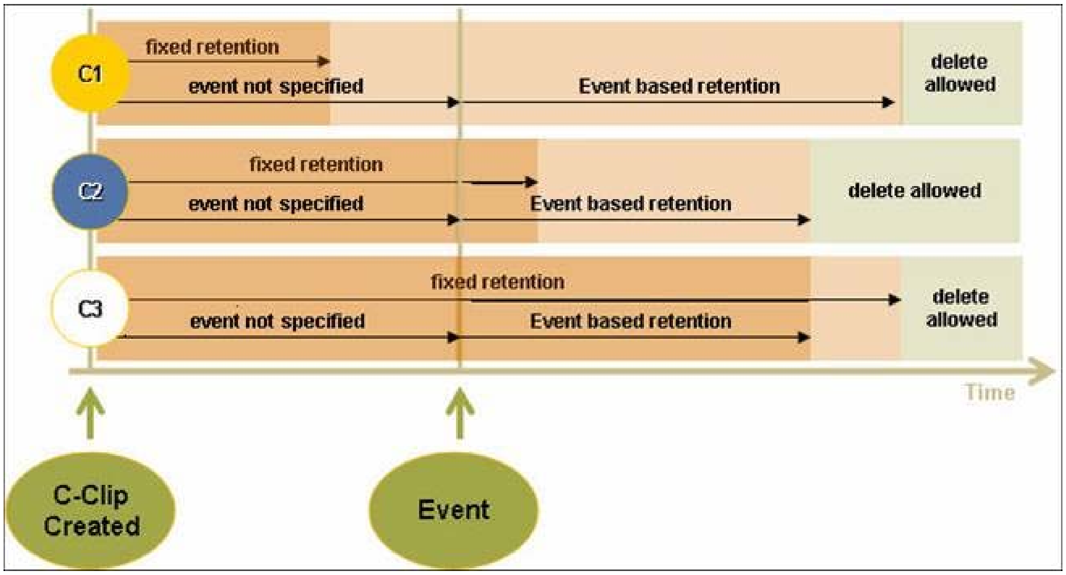


Figure 1. Event Based Retention

Litigation Hold

Litigation Hold allows applications to temporarily prevent deletion of the CDF. Litigation Hold can be used for data that is subject to an official investigation, subpoena, or inquiry and that may not be deleted until the investigation is over. Once there is no need to Hold the data anymore, the Litigation Hold can be released by the application that enabled the Hold. The application may place and remove Litigation Hold at the CDF level; one CDF can be under up to 100 Litigation Holds.

When using Litigation Hold, the CDF life-cycle is as follows:

1. **Create:** The application creates a new CDF and provides a regular and/or Event Based Retention period.

2. **Set Hold:** The application (can be different from the application writing the CDF) puts the CDF on Hold.

3. **Release Hold**: The application (can be different from the application writing or Holding the CDF) releases the CDF.

4. **Delete:** When the application tries to delete the CDF, the following conditions must be satisfied:
   - Fixed and Event Based Retention have expired.
   - There are no Litigation Holds outstanding on the CDF.

Notes:

Privileged Delete cannot *delete a CDF under Litigation Hold.*

Being under Litigation Hold does not *"stop the clock" for the CDF, that is, the period a CDF is under Litigation is* not *added to the initial retention period.*

Applications that wish to make use of the LH feature must have the (h) capability enabled and use SDK 3.1 or later.

Figure 2 shows the three possible scenarios for a CDF being put under Litigation Hold:

• C1 already had the retention expired when put under Hold.

• C2 had the retention period expire during the Hold.

• C3 still was under retention after release of the Hold.

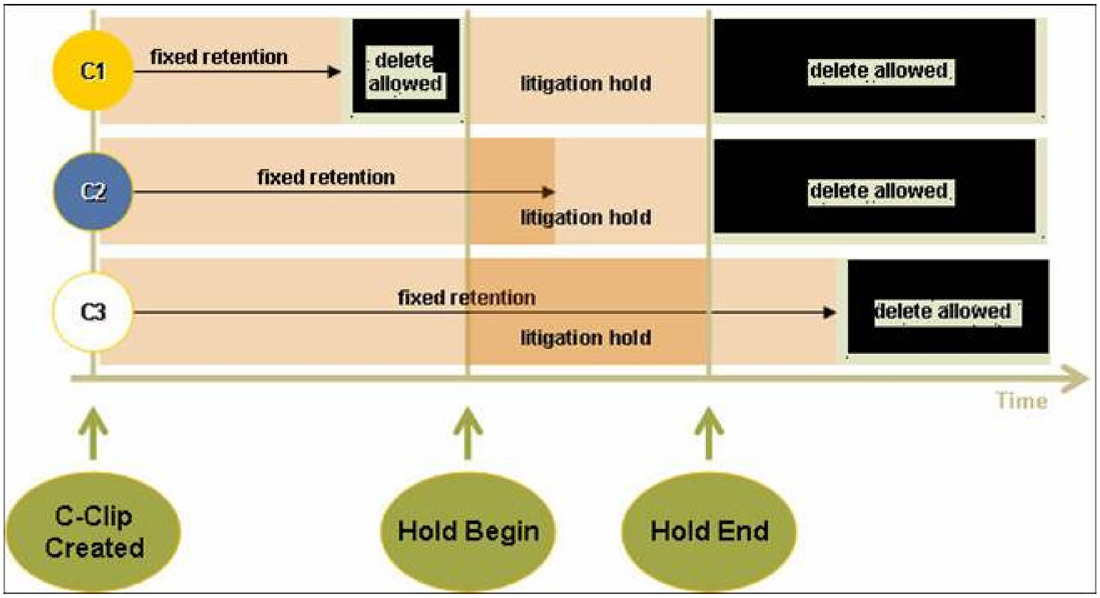


Figure 2. Litigation Hold

Min/Max Governor

The Min/Max Governor feature allows the system administrator to specify a minimum and maximum value for the retention period on a per-pool basis, one for fixed retention and one for variable retention. When an application tries to write a CDF to a pool with a retention period that falls outside the min/max settings, an error will be thrown.

The SDK and EMC Centera will not accept any CDFs with a retention period that does not match the Min/Max Governor constraints:

- Enforce the presence of retention information, that is, do not accept CDFs without retention period or class.
  - Applies to pre-SDK 3.1 – SDK 3.1 will always enter a retention period if not provided using the default retention period, as discussed in the next section.
- Default retention periods must also be within the Min/Max setting; unlike the default retention period, the CDF is not changed by applying the minimum or maximum rules.
- Enforce a minimum retention period – not for classes, see notes.
- Enforce a maximum retention period – not for classes, see notes.
- If any constraint is not met, the write of the CDF fails.

Notes: Default retention must be within the Min/Max settings – if not, a warning is issued.

When using retention classes, the min/max settings are not enforced.

When creating a CDF under EBR, and the application does not specify a fixed retention policy, a 0 retention period is added instead of using the default retention and the min/max is not enforced.

CDFs being restored do not check these constraints.

Remote management options

System administrators and EMC Service use tools such as the EMC Centera Command Line Interface (CLI) and EMC Centera Viewer (CV) to configure and support the cluster. In some cases, EMC Service will need direct access to the EMC Centera platform.

When EMC Service needs access to an EMC Centera cluster remotely, there are two options available:

- Modem: EMC Service engineers can connect to an EMC Centera cluster via a modem from the EMC VPN. For this connection a client-side software handshaking occurs between the EMC Centera and the system of the EMC engineer. The negotiation of the handshaking is encrypted (40-bit, proprietary method that is session specific) and must be successful in order to establish a PPP session.
- EMC Secure Remote Support: This gateway solution provides IP-based, firewall-friendly connectivity from EMC to an EMC Centera cluster with extensive security and authorization controls available to the customer.

EMC recommends that the system administrator keeps the cluster locked at all times – by default all nodes are locked. By locking a cluster, remote access to the cluster – SSH and remote EMC service access to nodes – is disabled.

For service interventions, the nodes can be unlocked to allow remote access. Alternatively direct access through the Eth2 port on a storage node is permitted.

While a lock command applies to the cluster, the unlock command can unlock either all nodes within a cluster or individual nodes.

To support network segmentation, CentraStar 4.0 introduces two new node roles in addition to storage and access roles: the management role and the replication role. By assigning the individual node roles to distinct nodes in the cluster, the different types of network traffic will be segregated. Management traffic (management commands from management applications such as EMC Centera Console, CLI, or EMC

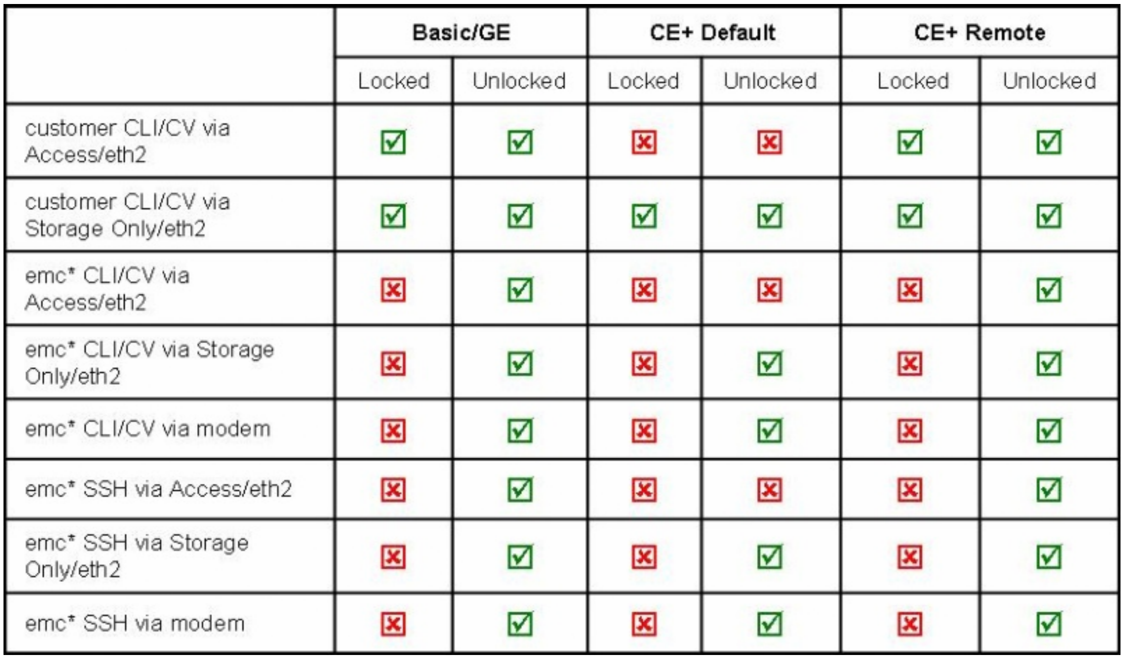
Centera Viewer, SNMP events, emails, and more) will be sent through the nodes with the management role.

Notes: From CentraStar 3.1.3 onward, management connections are secured using the TLS/SSL protocol. This requires the installation of X.509 public key certificates on both the cluster and the client machine.

For maximum security EMC recommends that modems are not connected to the cluster continuously but only for the duration of the service intervention.

Table 2 summarizes the different remote management options for the three EMC Centera models.

Table 2. Remote management matrix



	Basic/GE		CE+ Default		CE+ Remote	
	Locked	Unlocked	Locked	Unlocked	Locked	Unlocked
customer CLI/CV via Access/eth2	☑	☑	☒	☒	☑	☑
customer CLI/CV via Storage Only/eth2	☑	☑	☑	☑	☑	☑
emc* CLI/CV via Access/eth2	☒	☑	☒	☒	☒	☑
emc* CLI/CV via Storage Only/eth2	☒	☑	☒	☑	☒	☑
emc* CLI/CV via modem	☒	☑	☒	☑	☒	☑
emc* SSH via Access/eth2	☒	☑	☒	☒	☒	☑
emc* SSH via Storage Only/eth2	☒	☑	☒	☑	☒	☑
emc* SSH via modem	☒	☑	☒	☑	☒	☑

SNMP

The Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks. It allows EMC Centera to communicate status, warning, and critical information to storage management software such as the EMC ControlCenter® family.

The ConnectEMC agent uses an SMTP connection to send health information and alerts to EMC. The XML messages are encrypted and uu-encoded using FIPs 140 compliant encryption standards with AES (Advanced Encryption Standard) 256-bit strong encryption to meet the U.S. Department of Defense standards for security.

Note: By default, SNMP is disabled for CE+ clusters but it can be enabled by the system administrator.

Remote management access on CE+ clusters

With CentraStar 4.0 the customer has the option to configure a separate network for management and be able to manage the EMC Centera from that network provided that the customer has verified this does not violate his compliance requirements

For CentraStar 3.1 an RPQ is required to manage EMC Centera from a separate management network provided there are nodes with only the storage role available to configure for this capability.

To manage a CE+ cluster running CentraStar 4.0, you can connect the CLI to a node that has the management role and/or storage role and no other external node roles (replication and access). If the node only has the storage role, you need to connect directly to the ETH2 port of that node.

CE+ clusters will not allow a management connection over the network to nodes that are also used for access and/or replication traffic. Monitoring functionality such as email home (SMTP), syslog, and SNMP will however be possible on these nodes using the management role.

Conclusion

EMC Centera enforces organizational and application policies for information retention and disposition intrinsic in storage—and by doing so completes the information chain of custody. It ensures corporate accountability and reduces the costs of legal discovery and litigation support—and it's easy to manage.

Automate your entire content lifecycle to mitigate the risk of noncompliance. You'll leverage full auditability at all stages of content creation, approval, and use while enforcing information retention and disposal.

References

- *EMC Centera Online Help*
- *EMC Centera SDK Version 3.2 API Reference Guide*
- *EMC Centera Console Version 2.2 Setup Guide*
- *EMC Centera SDK Version 3.2 Programmer's Guide*
- *EMC Centera Server Version 4.0 Release Notes*
- EMC Centera Family page on EMC.com
- "Data storage compliance's impact on storage product choices" on SearchStorage.com
- The Sarbanex-Oxley Act (SOX) on the SEC website
- "Compliance (regulation)" on Wikipedia.com

Appendix: The compliance veto

On a Basic model, no vetoes are imposed. Clip and BLOB Purge are allowed.

Note: The Purge functions in the EMC Centera SDK are deprecated, are not supported, and are not recommended except under supervision by EMC Centera Corporate Systems Engineering.

On a Governance model, BLOB Purge is vetoed and Clip Purge is translated and processed on the server as a Privileged Delete. This requires the application to have read (r), purge (p), and privileged delete (D) capabilities.

On a Compliance Edition Plus model, the purge (p) and privileged delete (D) capabilities will always be vetoed by CentraStar, irrespective of the settings of access profile capabilities or cluster and pool masks.

This results in Purge BLOB, Purge Clip, and Privileged Delete calls being vetoed. In addition, a CE+ cluster will refuse access through the access nodes for any profile that has been granted a management role other than the monitor role. This allows profiles to perform remote monitoring and reporting but not remote management or service via the access nodes.

Table 3 summarizes the Centera compliance veto.

Table 3. Compliance veto matrix

Centera API Call	Basic	GE	CE+
BLOB Purge	**Allowed** Requires (r)[1] and (p)[1]	**Vetoed**	**Vetoed**
Clip Purge	**Allowed** Requires (p)[1] and (D)[1]	**Allowed** Processed as Privileged Delete Requires (p)[1] and (D)[1]	**Vetoed**
Privileged Delete	**Allowed** Requires (p)[1] and (D)[1]	Yes Processed as Privileged Delete Requires (p)[1] and (D)[1]	**Vetoed**

[1] EMC Centera capabilities required by the application