



CATE Storage and Backup Engineering
Citigroup Architecture and Technology engineering

IBM XIV Storage Array

R11.4.2

CSBE-14020-SG

Solutions Guide

1.4

©Citigroup Inc. 2015, All Rights Reserved.

This document contains material confidential to Citigroup. The contents are protected by specific employee and contractor agreements regarding confidentiality. Reproduction for distribution outside of Citigroup is prohibited.

1. Version Control

Version	Date	Author	Reviewed	Comments
0.1	15-July-2014	Scott Torgerson	Ludwig Derodel, Richard Rupp, Dan Meredith, Scott Bailey	Peer Review
0.5	30-July-2014	Scott Torgerson	Global Stakeholders	RFC
1.0	12-Sep-2014	Scott Torgerson	Global Stakeholders	Production Release
1.1	11-Dec-2014	Scott Torgerson	Ludwig Derodel	Added back out plan as per audit findings
1.2	27-Jan-2015	Scott Torgerson	Ludwig Derodel	Added minor changes for HPNA rules for Tivoli and SEMs
1.3	4-Feb-2015	Scott Torgerson	Ludwig Derodel	Revised back out plan
1.4	15-Apr-2015	Scott Torgerson	Global Stakeholders	Updated XRSC Version for production issue.

2. Legal Notice

Information contained herein is for Internal Use and may be used only for business purposes authorized by Citigroup.

CITI, CITIBANK, CITICORP, and CITIGROUP are trademarks and service marks of Citicorp and are used and registered throughout the world. Citibank, Citicorp, Citigroup and their subsidiaries also claim rights in certain other trademarks and service marks contained in these pages.

3. Contact

Please address any comments or questions regarding the information contained in this document via email to the *CATE Storage mailto:*CATE Storage and Backup Engineering and Backup Engineering distribution list.

4. Latest Versions

It is recommended that the latest version of the document be used from the CSBE website at the following URL:
<http://catecollaboration.citigroup.net/domains/platstor/gdse/products/default.aspx>.
Newer versions may include certification on additional platforms, or comments on issues discovered after deployment.

5. Table Of Contents

1. VERSION CONTROL	2
2. LEGAL NOTICE.....	3
3. CONTACT.....	3
4. LATEST VERSIONS	3
5. TABLE OF CONTENTS	4
6. EXECUTIVE SUMMARY	7
7. SCOPE	8
7.1 MAJOR ENHANCEMENTS AND FIXES IN THIS CERTIFICATION	8
7.2 PLANNED COMPONENT AND FUNCTIONALITY MATRIX.....	8
7.3 FUNCTIONALITY IN SCOPE	9
7.4 FUNCTIONALITY NOT IN SCOPE	9
8. PLANNING STEPS FOR NEW INSTALLS	10
8.1 PRE-INSTALLATION PLANNING STEPS FOR NEW INSTALLS	10
8.2 ORDER WINDOWS 2008 R2 MANAGEMENT STATION	10
8.3 ORDER NEW LINUX XRSC, ISIS, AND XCLI, MANAGEMENT STATION VM....	10
8.4 REQUEST LDAP FID ACCOUNT.....	11
8.5 READ-ONLY SERVICES FID ACCOUNT	11
8.6 REQUEST vCENTER PLUG-IN FID ACCOUNT	12
8.7 PHYSICAL INSTALLATION AND TDA MEETING	12
8.8 FIREWALL/CEP ORDER/INSTALLATION CONFIGURATION.....	12
8.9 XIV CABLING	13
8.10 VALIDATE VMWARE WEBCLIENT ROLE AND FID.....	16
8.11 ORDER GOOGLE CHROME OF ANY DESKTOPS THAT WILL MANAGE ISIS	18
9. UPGRADE CHECKLIST FROM PREVIOUS XIV RELEASE	19
9.1 PLANNING STEPS CHECKLIST.....	19
9.2 WINDOWS MANAGEMENT STATION CHECKLIST	19
9.3 XIV ARRAY CHECKLIST	19
9.4 LINUX MANAGEMENT STATION CHECKLIST (CLI, ISIS, XRSC)	20
9.5 BACK-OUT PLAN.....	21
10. INSTALLATION.....	22
10.1 WINDOWS MANAGEMENT STATION INSTALLATION.....	22
10.1.1 Remove Old XIV Management Tools (<i>Upgrades Only</i>)	22
10.1.2 Windows XIV Management Tools Installation	22
10.1.3 Windows Wrap Executable Installation (<i>Optional</i>)	23
10.1.4 Initial GUI Array Discovery (New Installs).....	24
10.1.5 GUI Remote Enhancement Settings.....	24
10.1.6 Group Arrays on the GUI Display	25

10.1.7	Configure GUI Properties Sharing	26
10.1.8	XIV Performance Package Installation	28
10.2	LINUX MANAGEMENT STATION INSTALLATION	29
10.2.1	Linux Wrap Executable Installation (<i>Optional</i>)	29
10.2.2	Install XRSC Proxy	30
10.2.3	Configure and Start XRSC Proxy	31
10.2.4	Remove Previous XIV CLI (<i>If Necessary</i>).....	32
10.2.5	Install XIV CLI (XCLI)	32
10.2.6	Install ISIS	33
10.2.7	Configure LDAP for ISIS.....	34
10.2.8	Configure CLI Protect.....	37
10.2.8.1	Test CLI	37
11.	CONFIGURATION.....	38
11.1	INITIAL ISIS CONFIGURATION	38
11.1.1	Change Initial admin password	38
11.1.2	Adding XIV Arrays to ISIS	39
11.1.3	Add VMWare WebClients to ISIS	39
11.1.4	Giving WebClients Access to XIV Pools.....	40
11.2	INITIAL XIV ADMIN PASSWORD CHANGE	40
11.3	CHANGE SNMP COMMUNITY STRINGS	41
11.4	LDAP CONFIGURATION.....	41
11.5	XIV XRSC SUPPORT CENTER DEFINITION	44
11.6	POOL CREATION	47
11.7	HOST/CLUSTER CREATION ON XIV	47
11.8	LUN CREATION ON XIV USING vCENTER WEBCLIENT PLUG-IN.....	48
11.9	EVENT NOTIFICATION	50
11.9.1	Creating a Tivoli or SAN Support DL Destination	51
11.9.2	Creating Tivoli or SAN Support DL Rules.....	52
11.9.3	Validate Aperture Fields	53
11.9.4	Validate Correct XIV IP in SMRWEB.....	53
11.9.5	Adding New Events to Tivoli Include List.....	54
11.10	CHARGEBACK AND CAPACITY REPORTING	55
11.11	PERFORMANCE REPORTING.....	55
11.12	SANSCREEN INTEGRATION.....	56
11.13	LOG REVIEW AND RECONCILIATION (SEMS)	57
11.14	EMC SRM INTEGRATION	58
11.15	HP NETWORK AUTOMATION (HPNA) INTEGRATIONS.....	58
11.15.1	Setup HPNA Destination Groups (Tivoli and SEMs).....	58
12.	BEST PRACTICES	60
12.1	ARRAY OVER-SUBSCRIPTION.....	60
12.2	STORAGE POOL CREATION.....	60
12.3	POOL THRESHOLD ALERTING	60
12.4	POOL LOCKING	60
12.5	VMWARE ZONING.....	61

12.5.1	Zoning With 4 HBA Ports Per ESX Server	61
12.5.2	Zoning With 2 HBA Ports Per ESX Server	62
12.6	LUN CREATION	62
12.6.1	Decimal (Base 10), Binary (Base 2), and Block Options	62
12.6.2	XIV Rule of 17 GB	63
12.7	LUN SIZING	63
12.7.1	LUN Sizing using vCenter WebClient Plug-in	63
12.7.2	Data Migrations	63
12.8	ISIS APPLICATION	64
12.9	LUN NAMING	64
12.10	REMOTE VENDOR SUPPORT	64
12.11	HOST ATTACHED KITS (HAK)	65
12.12	VAAI DRIVER SUPPORT	65
12.13	IBM XIV PLUG-IN FOR VMWARE vSPHERE WEBCLIENTS	66
12.14	HOST MULTI-PATHING OPTIONS	66
12.15	PROVISIONING	66
12.16	DE-PROVISIONING	66
12.17	LDAP ROLE MAPPING	67
12.18	XIV CROSS-DOMAIN LDAP AUTHENTICATION	67
12.19	IBM RAID CONFIGURATION (RAID-X)	67
12.20	WRAP EXECUTABLES	68
13.	OPERATIONAL PROCEDURES	70
13.1	BACKING UP ISIS CONFIGURATION	70
13.2	RESTORING ISIS CONFIGURATION	71
13.3	UPGRADING FROM OLD vCENTER PLUG-IN TO WEBCLIENT PLUG-IN	72
14.	SECURITY CONSIDERATIONS	73
14.1	XRSC FINDINGS	73
14.1.1	APP009, APP011, APP013, and APP017 – Password Policy	73
14.1.2	APP044 and APP098 – Non EATDS Approved Solution	74
14.2	XIV AND GUI FINDINGS	74
14.2.1	CVA 2056 – Low Encryption	74
14.2.2	CVA 2055 – SSLv2.0 Access	74
15.	APPENDICES	75
15.1	APPENDIX “A” – XIV EVENTS SENT TO TIVOLI	75
15.2	APPENDIX “B” – CLI INITIAL XIV CONFIGURATION	76
15.3	APPENDIX “C” – CURRENT XIV SPECIFICATIONS	80
16.	REFERENCES	81

6. Executive Summary

The IBM XIV Storage System is a scalable enterprise disk storage system that is based on a grid of standard off-the-shelf hardware components. The primary components of the IBM XIV Storage System are known as modules. Modules provide processing, cache, and host interfaces and are comprised of “off the shelf” Intel based systems.

The XIV grid architecture attempts to make use of parallelism to allocate system resources evenly at all times and scale seamlessly, without the need for complex, time-consuming tuning and configuration. The XIV Storage System is based on a distributed architecture of interconnected modules, each with its own multi-core CPU, large cache and high-density SAS near line disk drives working in parallel to serve data to client applications. Every data volume is randomly spread across all modules and disks in the system, and the aggregate power of the entire system is continually available to every application. The XIV system presents this collection of disks as a single large data store on the storage network. The modules communicate with each other over an internal redundant network based on InfiniBand technology.

The system stores data by breaking it down into 1 megabyte chunks called partitions, each mirrored for redundancy to another module. The system distributes all the partitions automatically and uniformly across all the disks by means of a pseudo-random distribution algorithm. The system also distributes the application load across all system modules uniformly, putting the aggregate power of all modules at the service of all requests concurrently. By doing so, IBM *claims* the XIV can avoid the performance and reliability risks that can plague traditional clustered controller designs.

Based on the above factors, the XIV Storage array will continue to be certified for production use in Citigroup. *It has also been determined and agreed upon that the only area of production certification will be for ESX (LVM) environments at this time. Support for ALL other operating systems will be not be supported at this time.*¹

¹ The GRMAS application has been deployed on XIV Storage and support will continue for the as long as the application remains on XIV.

7. Scope

The scope of this project is to certify new operational versions of software management tools and microcode for the IBM XIV Generation 3 Storage Array.

7.1 Major Enhancements and Fixes in this Certification

- Fix for the Open SSL Heartbleed bug
- Fix for space reclamation in VMWare
- Addition of ISIS layer to accommodate new VMWare WebClient
- Addition of HPNA for automated SBCC
- Addition of EMC SRM on XIV
- New versions of Microcode and Management tools

7.2 Planned Component and Functionality Matrix

Component Matrix	
XIV Type / Model	2812/114
XIV Firmware/Microcode	11.4.2.a ²
Disk Drives	3TB NL SAS 7200RPM
Management Interface (GUI) ³	4.3.1 Build 1
Management Interface (CLI)	4.3.1 Build 1
Vendor Remote Access ⁴ (XRSC)	1.3.1.1 ⁵
ISIS (IBM Storage Integration Server) ⁶	1.2.1
XIV vCenter Plug-in	5.2.2 ⁷
VMWare WebClient Plug-in	1.2.1.17 ⁸
VMWare WebClient Version	5.5

² This version of microcode contains a fix for the SSL Heartbleed Bug.

³ At this time it is planned to have the XIV Management GUI packaged for the Windows Platform only.

⁴ For this version of XRSC, the Linux server holding XRSC will need to be rebuilt to RHEL 6.X SOE build so that the ISIS software can co-exist with XRSC.

⁵ This is an updated version of XRSC to resolve a production certificate issue.

⁶ ISIS is a new layer that needs to be implemented to accommodate the new VMWare vSphere WebClient plug-in.

⁷ This is considered the old plug-in that was certified first. As VMWare instances are updated from the vCenter application to the WebClients, administrators must also upgrade to the WebClient plug-in.

⁸ This new WebClient plug-in will not have to be packaged and loaded for vCenter and longer. As WebClients are added to ISIS, the associated vSphere WebClients will automatically load the XIV extension from the ISIS server. To run the old vCenter Plug-in on this XIV release will still require loading the previous vCenter plug-in.

7.3 *Functionality in Scope*

Below is a list of items that will be in scope for this phase of the XIV certification. All configuration instructions and settings for this certification will be recorded in the Solutions Guide document (CSBE-14020-SG), and all test results will be recorded in the Release Notes document (CSBE-14020-RN).

- Installation / Configuration
- Zoning and Provisioning
- Management Interfaces⁹
- Thin Provisioning / Over Subscription¹⁰
- ESX Platform Integration¹¹
- Event Notification (Tivoli)
- Vendor Remote Access (XRSC)
- IBM Storage Integration Server (ISIS)
- HPNA Testing for automated SBCC
- EMC SRM integration
- VMWare WebClient integration
- SANscreen Integration
- Data Migration¹²
- Performance Reporting
- SAA Standard Build and SBCC

7.4 *Functionality not in Scope*

Functionality that will not be considered in scope for this certification are listed below.

- Replication / COB
- All non ESX SAN Stacks and multi-pathing
- Snapshots

⁹ The complete management interface will be packaged for the Windows platform but only the XCLI will be packaged for the Linux platform.

¹⁰ All over provisioning will be done at the VMWare level. Only Regular XIV pools will be given to VMWare LVM environments.

¹¹ Only the ESX SAN Stack is planned in scope for this certification. All other platform SAN Stacks are on hold until pending other use cases for XIV.

¹² All data migration will be handled at the VMWare level with Storage vMotion.

8. Planning Steps For New Installs

8.1 Pre-Installation Planning Steps for New Installs

There are several planning steps that should be initiated as soon as new XIV Storage Array is ordered. Without any escalation these steps will take anywhere from 7-12 weeks and therefore should be started well prior to the delivery or planned installation of the new XIV array. Each item on the checklist below is a hyper link in this document with a more detailed description for each of these pre-installation steps.

- ✓ [Order Windows 2008 R2 Management Station VM \(if necessary\)](#)
- ✓ [Order Linux RH5.X 64bit CLI Management Station VM \(if necessary\)](#)
- ✓ [Request LDAP FID Account \(if necessary\)](#)
- ✓ [Request Read-Only Services FID Account \(if necessary\)](#)
- ✓ [Request vCenter Plug-In FID Account \(if Necessary\)](#)
- ✓ [Schedule IBM XIV TDA Meeting](#)
- ✓ [Order CEP and Request Specific Open Ports \(if necessary\)](#)
- ✓ [Make XIV Cabling Request](#)
- ✓ [Validate VMWare WebClient FID and Role](#)
- ✓ [Order Chrome for ISIS managers](#)

8.2 Order Windows 2008 R2 Management Station

In order to manage the XIV Storage Array a Windows server or VM will need to be in place to hold the management tools (GUI, XCLI, and XIV-TOP). If a site already has XIV storage arrays this management server should already be in place and this step can be skipped. If a site does not have XIV arrays this server should be ordered when the XIV is ordered. Once the server is in place on the floor the Windows [Management Station Installation section](#) of this document should be used to put the management applications in place.

The Windows server that will act as the XIV management server should be a Windows SOE standalone server or VM running ***SOE Build Windows 2008 R2***. The server hardware or VM should be at minimum dual core or equivalent with at least 2 GB of memory and 300MB or free disk space.

8.3 Order NEW Linux XRSC, ISIS, and XCLI, Management Station VM

The Linux Management Station VM will only have the XCLI (no GUI) executables installed for managing the XIV arrays. The XRSC proxy used for remote vendor support and the ISIS software used to support the new VMWare WebClient plug-in should also be loaded on this same VM. The requested VM should meet the following requirement.

- (4) vCPU's
- 8GB Memory
- 102GB Free **SAN**¹³ disk space
- SOE Build RHEL 6.3 or higher (64-bit)

A Linux VM for holding XCLI, XRSC, and ISIS should be installed for each data center containing (2) or more XIV Arrays.

8.4 Request LDAP FID Account

In order to configure LDAP on XIV it is required to have an AD functional/bind account created (FID). Any existing storage functional/bind AD account can be used if one is already created for other storage platforms (Ex: CLARiiON, VNX, etc.). However, the LDAP FID account should NOT be part of any AD groups and it should have its password set to never expire. If the storage administrator is going to create a new account it should follow the naming convention shown below:

<region>_svr_storage
Example: nam_svr_storage

Regional administrators will have to use Citi Market Place (CMP) to get an XIV LDAP Bind FID ordered and created.

8.5 Read-Only Services FID Account

In addition to the LDAP FID account described in the previous section, another FID account must also be created that will act as a read-only services account. This account should be added into the Regional AD read-only Group that will access the XIV array and have its password set to never expire.

Once this FID is added to the all read-only groups accessing the XIV it should be used for the following: SANscreen access, HPNA, Netuitive, EMC SRM, or any Chargeback Reporting servers remotely accessing the XIV to pull data, and all batch processing scripts that require a login on the XIV. The new account should use the following naming convention shown below:

<region>_san_view
Example: nam_san_view

¹³ For this VM SAN disk space should be requested as the Database that maintains ALL associations from XIV Pools to VMWare WebClients will be stored here. All reporting data for ALL VMWare LVM and reporting environments will also pull data from this location.

8.6 Request vCenter Plug-In FID Account

A FID should also be requested for use with the ISIS Array Credentials. This FID will be used when adding XIV Arrays into ISIS, and it will also be used to determine where to send log reconciliation events. The FID must have the name **vmwplugin** in order for [ArcSight log reconciliation](#) to occur correctly. Any XIV events that come to ArcSight with this FID name associated with them will be ignored and reconciliation will be completed using TEARS.

As part of the MP request the FID should have the following fields set as shown:

Is this an interactive ID: No How is Password Managed: Managed by Authorized User Account Type of FID: Process - Application Enter FID name: vmwplugin Set Password To Never Expire: Yes User Cannot Change Password: Yes
--

Since the password will be set to never expire, the password that will be assigned to the FID should also be given to the team creating the FID.

Once created, the FID then needs to be added into the regional XIV admins group in AD so that it can be used to [add XIV Arrays to ISIS](#).

8.7 Physical Installation and TDA Meeting

The physical installation of the XIV array is completed by an IBM Site Support Rep (SSR) working in conjunction with Citigroup lab or data center personnel. The IBM process used to get an XIV physically installed is the pre-install TDA (Technical delivery Assessment) which includes a questionnaire and a meeting between IBM and the Citigroup lab or datacenter personnel. When an XIV array is ordered for a Citigroup datacenter, an IBM TDA meeting should be scheduled, and once completed, IBM will give a date for their SSR to come in and do the complete physical installation of the XIV array.

NOTE: When giving TDA information, a valid Citigroup email account (not DL) must be given for the from address . Anything other than user@citigroup.com will result in failure for all XIV Call Home attempts.
--

8.8 Firewall/CEP Order/Installation Configuration

All XIV Management ports in a datacenter should be located behind a datacenter internal Firewall/CEP. As such, multiple proxy server and management servers should be configured to have access through the firewall to the XIV management ports. If a Firewall/CEP exists then new XIV arrays just need to be installed on

that segment. If a Firewall/CEP does not exist, it should be ordered when the order is placed for the XIV arrays. When ordering the Firewall/CEP, the following ports and rules will need configured to allow management and vendor remote support (XRSC) to the XIV management ports through the firewall.

Name	Outbound From XIV	Type	Incoming to XIV	Destination/Source
LDAP	389, 636	TCP		Regional LDAP Servers
SNTP	123	UDP		Regional NTP Servers
DNS	53	TCP UDP		Regional DNS Servers
SMTP	25	TCP		Regional SMTP Server
XRSC Proxy	25000	TCP		All Linux XRSC Proxy servers ¹⁴
CIM/SMI-S	5988, 5989	TCP	5988, 5989	Regional SRM XIV Collector
SNMP	162	UDP		Regional Tivoli and SEMs Servers
GUI/CLI	7778	TCP	7778	1 - All XIV IP management ports 2 - SOE GUI and CLI Servers (even those from other datacenters) 3 - Regional SANscreen Servers 4 – vCenter Servers 5 – Regional/Global HPNA Servers 6 – Datacenter ISIS Server VM

8.9 XIV Cabling

The XIV array will require (3) IP management port cables plugged into new or existing firewall (CEP) segments and will be used to handle all management traffic. FC cables should be connected to 8Gb FC infrastructure in any datacenters that support it. If the datacenter does not have 8Gb infrastructure then the FC cables can be connected to the standard 4Gb SAN infrastructure, but should be upgraded to 8Gb as soon as available.

The following diagrams depict how the XIV Array should be cabled when connecting to a 1, 2, 3, or 4 SANs.

Note: When cabling the XIV to 2 or 4 SANs, ports 4 on each I/O module will have to be changed from an initiator to a target. By default port 4 on each I/O module is setup as an initiator and designated for Array Based Migrations.

¹⁴ This list should include ALL Linux XRSC proxy servers in the region where the XIV is located. Currently it is planned that each region will have two of the Linux XRSC Proxy servers.

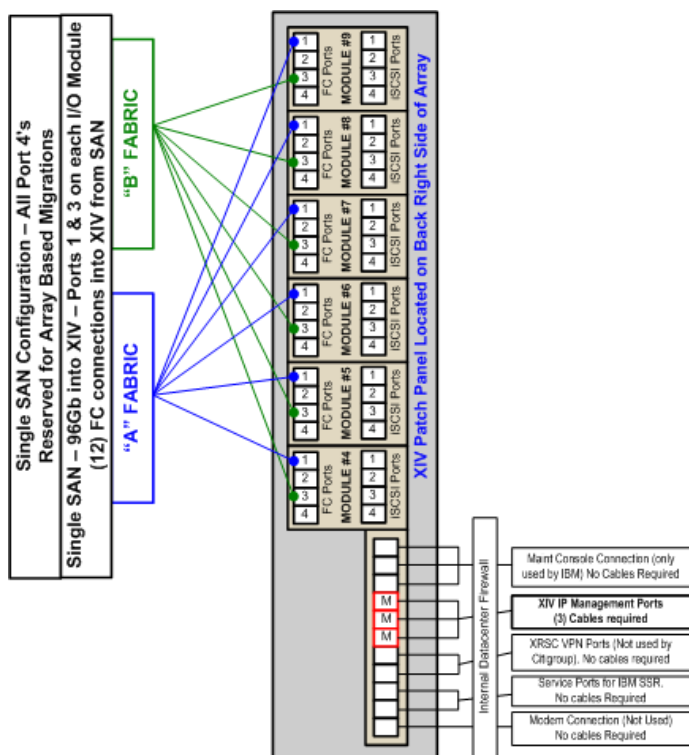


Figure 1 - Single SAN XIV Cabling Diagram

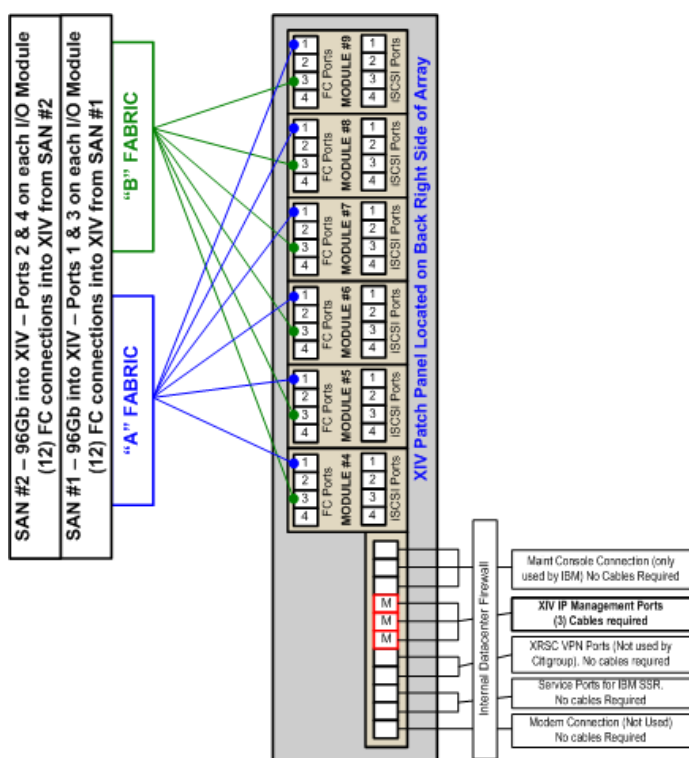


Figure 2 - Two SAN XIV Cabling Diagram

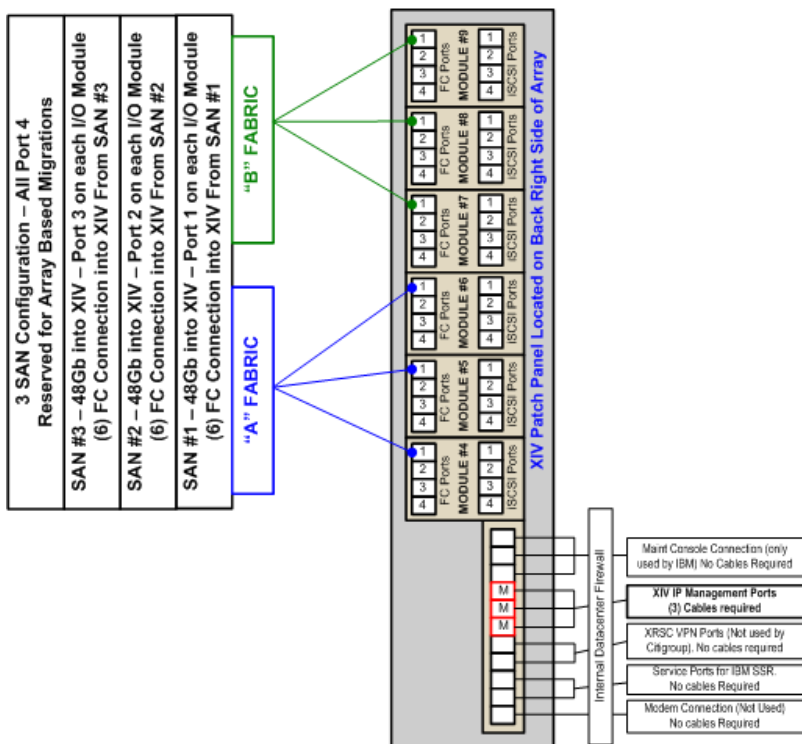


Figure 3 _ Three SAN XIV Cabling Diagram

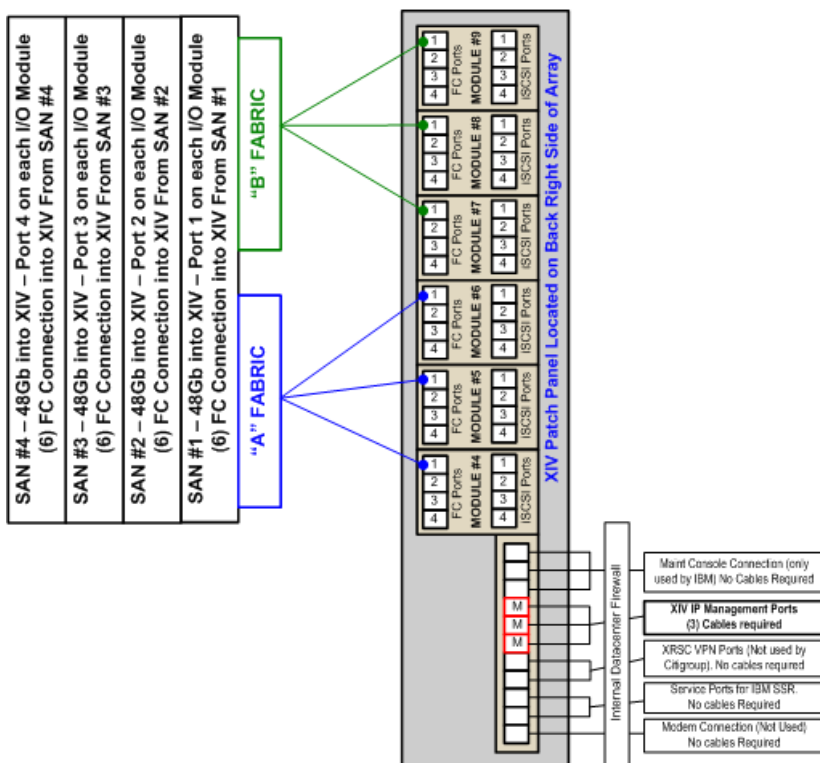


Figure 4 - Four SAN XIV Cabling Diagram

Note: In the above diagrams port 4 on all I/O modules will be reserved for Array Based Migration when cabling the XIV to a single SAN or when cabling to three SANs. When cabling to 2 or 4 SANs there is no ports available for Array Based Migrations.

8.10 Validate VMWare WebClient Role and FID

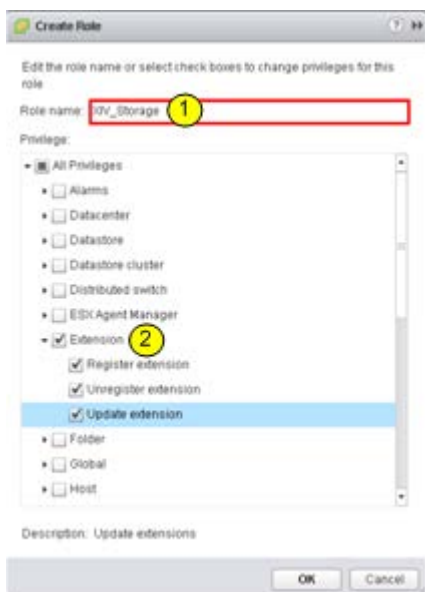
With the addition of the new VMWare WebClient and the new ISIS layer, the way in which an XIV pool is attached to a vCenter server has changed. All new WebClients have to be added into the ISIS server using a VMWare FID and Role with the required privileges. Once validated, the VMWare team will give the FID and password to the Storage Operations team so that they can add vSphere WebClients to ISIS and associate XIV Pools with vSphere WebClients.

The VMWare Operations Team should first create the “**xivisis**” FID for their region using the following options in CMP.

Is this an interactive ID: **No**
How is Password Managed: **Managed by Authorized User**
Account Type of FID: **Process - Application**
Enter FID name: **xivisis**
Set Password To Never Expire: **Yes**
User Cannot Change Password: **Yes**

It also needs to be validated that the VMWare Operations team has created an XIV_Storage role that contains the “xivisis” FID, and that the role has been placed at the vCenter server level for the associated vSphere Web Clients.

VMWare administrators creating the Role should use the following to get the new role created. At the main home screen of the WebClient, select “*administration -> Roles*” and then select the “*Create Role Action*” which appears as a “+”. Once the *Create Role Screen* appears the following should be selected for the following categories:



First, the VMWare administrator should enter the Role Name of **XIV_Storage**. Then for each of the following categories the following should be checked.

- **Extensions** – Register extension, Unregister extension, Update extension
- **Global** – Log event, Cancel task
- **Tasks** – Create task, Update task
- **Sessions** – Impersonate user
- **Host** – For this category Select **Configuration** and then check Storage partition configuration

Once the XIV_Storage role has been created, the VMWare administrator will now need to add that role with the “xivisis” FID at the vCenter level of each vSphere WebClient that will use XIV Storage as shown below.



- Select the appropriate vCenter server holding the WebClient
- Select the Manage Tab
- Select the Permissions Tab
- Select the Add Permissions icon (+). This will make the Add Permissions Screen appear.
- Add Permissions Screen (Not Shown) – Once the *Add Permissions* screen appears first select the users and groups on the left side. This will pop-up a new user and group screen and first the domain should be selected where the XIV resides. Then search for the “xivisis” FID and then

select “Ok”. Then on the right hand side of the Add Permissions screen select the “XIV_Storage” role and then select “OK”

Once all of the above has been completed by the VMWare Operations Team, the password of the *xivisis* FID should be given to the Storage Operations Team member who is adding the VMWare WebClients to ISIS.

8.11 Order Google Chrome of any Desktops that will manage ISIS

IBM ISIS is supposed to work with Internet Explorer 9 and above, Google Chrome 27.0 and above, or Mozilla Firefox 21.0 and above. However, while testing with Internet Explorer 9.0 it was found that not all items functioned properly. For this first release of ISIS it is recommended to use Google Chrome on any Desktops that will manage XIV arrays and VMWare WebClients in ISIS. Since older SOE Desktops builds did not come default with Google Chrome loaded, it may have to be ordered in CMP at the following URL for Global Desktop Software:

https://cmp.nj.smb.com/marketplace/control/product/~productId=47268_465603_GLOBAL#

When ordering Chrome the following fields should have the values list below:

- **Vendor or product name** – GOOGLE INC---Chrome(22713)
- **Application Version** – 31 [63504]
- **CTC Version** – 63504

NOTE: Although Internet Explorer 9 was found not to work with ISIS, IE10 was tested and did perform as expected. However, at the time of the writing of this document, IE 10 shows as “Skipped” in CMP and IE 11 shows as “Under Evaluation”. As a result no further testing was completed with ISIS running on the IE browser.

9. Upgrade CheckList from Previous XIV Release

The following sections will discuss the exact steps that need to be taken on each XIV component to upgrade it to the new version/release.

9.1 Planning Steps Checklist

- ✓ [Order New Linux Management Station VM](#) for ISIS.

- ✓ Add new [Firewall rules](#) for new features.

(Add new Rules for **Regional or Global HPNA Servers**)

(Add new Rules for **Regional or Global EMC SRM XIV Collectors**)

(Add new Rules for new **Datacenter ISIS Server**)

(Update **XRSC rule** to point at new Linux Management Station VM)

- ✓ [Validate VMWare XIV FID and Role](#) has been created.

(Validate that **Regional VMWare “xivisis” FID** has been created)

(Validate that **Regional VMWare “XIV_Storage” Role** has been created)

(Get password for “xivisis” FID)

- ✓ [Order Google Chrome for ISIS Manager desktops](#)

(Order Google Chrome in CMP for any desktop that will connect to and manage ISIS)

- ✓ Order [NEW AD Security Admin Role AD Group](#)

Note: This is new XIV functionality which adds a Security Admin Role. Because of [Known Issues discussed in the Release Notes document](#) it cannot be used at this time. However, since the role is required it must be defined so that needed changes to the LDAP config can be made for this Release. *Storage Administrators should add this AD group and point the XIV Security Admin Role at it, but NOT add any users to the group.*

9.2 Windows Management Station Checklist

- ✓ [Remove old XIV GUI](#)

(Remember to remove old GUI shortcut in C:\Users\All Users\Desktop)

- ✓ [Install new GUI](#)

- ✓ Import previous systems file (if necessary)

(This should not be necessary if upgrade is done properly)

- ✓ [Setup GUI Remote Enhancements](#)

- ✓ [Configure GUI Sharing Properties](#)

(-h dir and files should exist. Main thing here is to setup icon with -h for all users desktop)

9.3 XIV Array Checklist

- ✓ Have IBM update XIV code to 11.4.2.a

- ✓ Accept the new elicense

Note: This command is new and does not show up anywhere else in the document. After the microcode is loaded, use the following CLI command to accept the elicence on each XIV that gets it microcode updated. This can only be completed from the CLI.

```
XIV-7820031>>elicense_accept approver_name="Citigroup"  
version="xiv_license_v11.4.2.a"
```

Command executed successfully.

- ✓ Make XIV LDAP Change to accommodate ISIS LDAP Logins

Note: In LDAP configuration “User Credentials” tab change the “Service User DN” from a long name to a short name. Example:

Change “Service User DN” value **FROM**

CN=nam_srvc_storage,OU=Svc_Accts,OU=SAN,OU=INFRA,DC=nam,DC=nsroot,DC=net

Change “Service User DN” value **TO**

nam_srvc_storage

- ✓ Make [HPNA Changes for SEMS Destination](#)

Note: Currently SEMS may have two separate destinations defined in a SEMS Rule. All Regions should rename the rule to “SEMS” (if necessary) and change the name of the two destinations to “SEMS1” and “SEMS2” and then put them in a destination group named SEMS. This is for HPNA consistency.

- ✓ Make [HPNA Changes for TIVOLI Destination](#)

Note: Currently Tivoli may have two separate destinations defined in a Tivoli Rule. All Regions should rename the rule to “TIVOLI” and change the name of the two destinations to “TIV1” and “TIV2” and then put in a destination group named TIVOLI. This is for HPNA consistency.

- ✓ [Add new Support Center Definition](#)

Note: This step cannot be completed until the new Linux Management Station VM is built and XRSC has been installed configured and started on it.

(Point new Support Center at new Linux Management Station VM XRSC)
(Remove old Support Center definition)

9.4 Linux Management Station Checklist (CLI, ISIS, XRSC)

- ✓ Get [new Linux Management Station VM](#) built

- ✓ [Install XRSC Proxy](#) on new VM

(can use same /etc/xiv/proxy.conf file from old XRSC server)

- ✓ [Configure and Start XRSC Proxy](#)

- ✓ [Install XIV CLI](#)

- ✓ [Install ISIS](#)

- ✓ [Configure ISIS](#)

9.5 Back-out Plan

For all generations of XIV Storage Arrays, down grading microcode versions is not supported. As a result, there is no back-out plan. The only option is to use IBM support, processes, and procedures to fail forward on newly upgraded versions of microcode.

10. Installation

10.1 Windows Management Station Installation

The XIV GUI is a Java client that runs on Windows, Solaris, Linux, AIX, MAC OS or HP UX. The command line XCLI client is available for the same platforms, and also installs the required Python run-time environment. All actions available from the GUI can also be completed using the XCLI. The XIV management interfaces (XGUI and XCLI) will be required to run on SOE management servers that have access through a firewall (CEP) to the XIV IP management ports.

The management interface was found to run well with quick responses when run on a local desktop. However, when run across the network on an SOE management server via RDP is slowed considerably as most Java based apps do. Once the XIV Management GUI is loaded on the SOE management server, it will require that specific settings be changed to turn off animation and other GUI functionality that will speed it up to a more usable state. See [GUI Remote Enhancement Settings](#) section of this document for further details.

10.1.1 Remove Old XIV Management Tools (*Upgrades Only*)

If the Windows Management Station already has the XIV Management GUI, and a new version is being installed as part of an upgrade, the old version should be removed prior to installing the new GUI using the following steps.

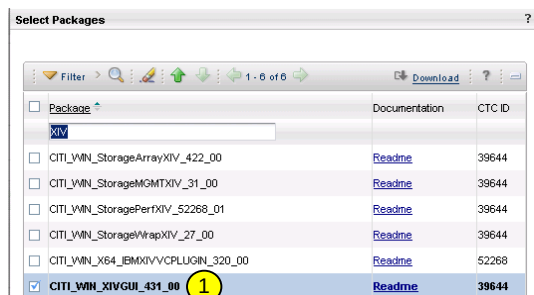
- Export the XIV Systems file – On the XIV GUI “*All Systems*” screen select the “*Systems*” tab and then select “*Export Systems File*” from the drop-down menu. Select a location and name for the file and save.
- Remove the old XIV GUI using *Control Panel* and *Programs and Features*
- Remove the shared XIV GUI icon with the –h option defined, from the C:\Users\All Users\Desktop location

10.1.2 Windows XIV Management Tools Installation

Note: If this is an upgrade from an older version of the GUI, the old GUI should be removed (via Control Panel) prior to loading the new one. Prior to removing the old GUI, an export of the current systems file should be made and stored on the GUI server. At the main GUI screen the administrator should select *System > Export Systems File* and select a name and location for the xml file to be stored.

Note: If a previous version of the XIV GUI exists on the management server it should be removed prior to loading the new version. After removal, if there is a shared XIV GUI shortcut in the C:\Users\All Users\Desktop directory it should also be removed from the directory and the desktop of the administrator user.

The XIV management tools can be installed on the Windows SOE management server using TPM and installing the CITI_WIN_XIVGUI_431_00 package.



The above TPM will simply drop the vendor executable file xivGUI-4.3.1-build1-win64.exe in the C:\tmp directory and it must then be executed.

If the new XIV GUI is installed in the same directory as the old version, the administrator will be warned that the new install will override the old install and the administrator should select “Ok”.

At the end of the install there is a check-box asking if the GUI should be launched. If this is a first time install of the XIV GUI on the management server the checkbox should be left checked and the administrator can go the [Initial GUI Array Discover section](#) of this document to start configuration.

Note: If a previous version of the XIV GUI existed prior to installing the new version, the administrator should uncheck this box and hit the finish button and then go to the [GUI Properties Sharing](#) section and continue the configuration.

10.1.3 Windows Wrap Executable Installation (Optional)

The Windows Wrap executables are no longer needed for running simple CLI commands because of the addition of the `-protect` option in the new XCLI. However, for administrators wishing to run large command files containing passwords like the Example given in [Appendix “B”](#) they can still be used. Further details about the wrap executables can also be found in the [Best Practices \(Wrap Executables\)](#) section.

The Windows [wrap executable](#) can be installed to run large command files by using TPM to install the CITI_WIN_StorageWrapXIV_27_00 package.



10.1.4 Initial GUI Array Discovery (New Installs)

The very first time the XIV GUI is launched the Add Managed Systems screen will appear. At this point all management port of an existing XIV Array needs to be entered as shown below.



Once an initial array has been added to the GUI, other arrays can be added from the main GUI screen by selecting the “Add System” icon as shown below.



10.1.5 GUI Remote Enhancement Settings

Without modification the XIV GUI has trouble running at an acceptable speed from a remote management station. The following GUI settings should be changed to remove animation that will allow the GUI to run at a higher speed. To make these changes launch the GUI on the remote management station and on the main screen select *Tools > Management*.

The following settings box will appear and the appropriate changes should be made as show the below. 1 – Change Dock Magnification to “none”, 2 – Change Show Tips to “No”, 3 – Change GUI Mode to “Low”, and 4 – Change Dynamic Menus to “Off”.



10.1.6 Group Arrays on the GUI Display

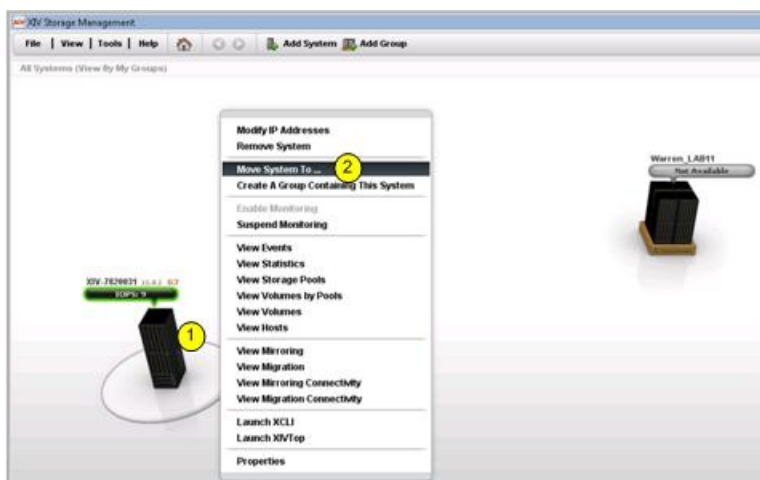
Once all arrays are discovered on the GUI in each datacenter, the XIV arrays should be put into datacenter groups. At the initial GUI login screen select the Add Group icon as shown below.



The following screen will appear and datacenter groups should be created using a naming convention similar to <Name>_<Type> (ex: SWDC or MWDC) as shown below.



Once the groups are created each XIV array should be put into the proper datacenter or lab group. On the same GUI screen where the new groups are displayed, right click on each XIV array and select "Move System To.." from the pull-down menu as shown below.



Select the group to add the XIV array to from the group pull-down menu. Do this for each array in the display until only group icons are displayed.



10.1.7 Configure GUI Properties Sharing

By default every user that logs into the Windows Management server and launches the XIV GUI will have their own GUI properties kept under the AppData\Roaming\XIV\GUI11\properties directory. Without setting this as a shared location it means that every user would have to populate their own GUI view with all arrays and groups.

To avoid the issue of having each user populate their own GUI views the following steps can be taken to share this information. These steps should be completed on each Windows management server **as administrator**.

Note: All the following steps should be completed for a new clean install. If the new GUI was as a result of an upgrade, then only Steps #1, #5, and #6 need to be completed because the arrays will already be populated in the GUI and the –h directory location will already be created with files in it.

1 – From the Windows start menu under the IBM XIV 4.3.1 folder, copy and create a desktop shortcut for the XIV GUI program.

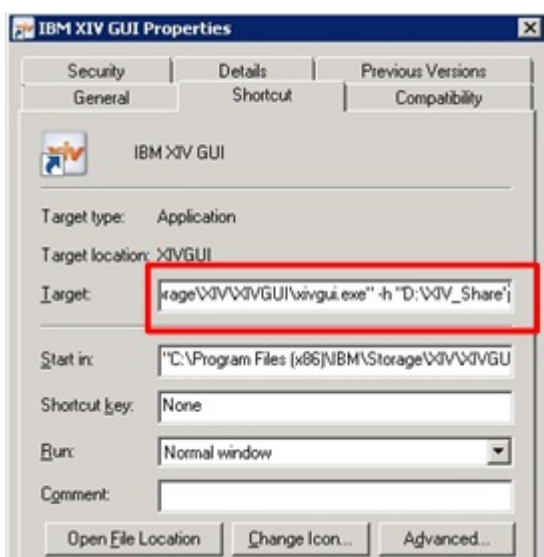
2 – Launch the XIV GUI using “admin” to login and [add all XIV arrays](#) into the GUI display. Once all arrays are added then [group the arrays](#) in the display by site/datacenter or whatever grouping is appropriate for the region.

3 – Create a directory where a common **xiv-systems.xml** file will be shared from (ex: D:\XIV_Share).

4 – From the main GUI screen Export the XIV systems file into the shared directory from the previous step (the file should be named xiv-systems.xml instead of the default)



5 – Edit the shortcut properties of the shortcut created in the earlier step to include [-h "Path of shared directory created above"]. Ex: "C:\Program Files (x86)\ibm\Storage\XIV\XIVGUI\xivgui.exe" -h "D:\XIV_Share"



6 – After the shortcut properties have been modified, the shortcut should then be copied into the **C:\Documents and Settings\All Users\Desktop** directory.

At this point all users that log into the Windows Management Station will have the same XIV GUI shortcut on their desktop and when launched will already contain all the systems and XIV groups.

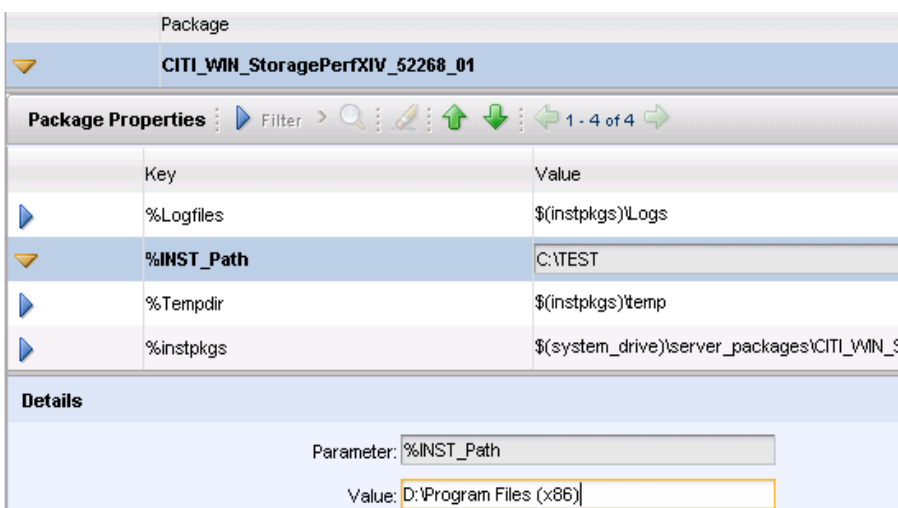
10.1.8 XIV Performance Package Installation

Currently the Performance Package is only used to generate performance data used to for long term historical purposes.

The XIV Performance Reporting Tools should be installed and configured on at least one Windows Management Station by using TPM to install the CITI_WIN_StoragePerfXIV_52268_01 package.



The administrator should set where they want the package to install in the package properties as shown below:



Once installed, the performance monitoring tools should be configured using instructions provided in the [XIV Performance Reporting Tools](#) section.

10.2 Linux Management Station Installation

The Linux Management Station VM (see [Planning Steps](#) for VM requirements), will contain the XIV CLI (no GUI) executables installed for managing the XIV arrays. The XRSC proxy used for remote vendor support and the ISIS software used to support the new VMWare WebClient plug-in should also be loaded on this same VM.

Once the Linux Management Station VM has been installed with the O.S., use the following sections of this document to install and configure all of the necessary XIV components.

10.2.1 Linux Wrap Executable Installation (*Optional*)

The Linux wrap executable can be installed on the Linux Management Station for administrators wishing to run large command files to initially configure XIV arrays (ex: [Appendix “B”](#)). For administrators not using this functionality on the Linux Management Station there is no need to install the wrap executables.

The Linux [wrap executable](#) can be installed by using yum to install the xiv_wrap_2.7 rpm package as shown below:

```
# yum install xiv_wrap-2.7
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package xiv_wrap.x86_64 0:2.7-A0 set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package                Arch             Version          Repository        Size
=====
Installing:
xiv_wrap                x86_64           2.7-A0           soe5products-testing 25 k
=====

Transaction Summary
=====
Install      1 Package(s)
Upgrade     0 Package(s)

Total download size: 25 k
Is this ok [y/N]: y
Downloading Packages:
xiv_wrap-2.7-A0.x86_64.rpm | 25 kB    00:00
Running rpm_check_debug
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing      : xiv_wrap                                1/1

Installed:
```

```
xiv_wrap.x86_64 0:2.7-A0
```

```
Complete!
```

Once installed the /opt/XV_Wrap_2.7 directory should be added to the Linux PATH variable.

10.2.2 Install XRSC Proxy

To install the XRSC Proxy, log into the Linux Management Station VM as root and first install the required redhat-lsb-core package. *Note that this package is installed with the `--nodeps` option intentionally.*

```
# cd /net/stealth/export1/home1.localhost/sw/Linux/xiv_3.0/XIV_Proxy_1.3.1

# ls
redhat-lsb-core-4.0-7.el6.x86_64.rpm
xivproxy-installer-rpm-1.3.1-b612.rhel6.x86_64.bin
xivproxy-installer-rpm-1.3.1.1-b1518.rhel6.x86_64.bin

# rpm -ivh redhat-lsb-core-4.0-7.el6.x86_64.rpm --nodeps
Preparing...                               ##### [100%]
   1:redhat-lsb-core                       ##### [100%]

# rpm -qa | grep redhat-lsb-core
redhat-lsb-core-4.0-7.el6.x86_64
```

After redhat-lsb-core is installed, the XRSC proxy should now be installed using the following command.

```
# cd /net/stealth/export1/home1.localhost/sw/Linux/xiv_3.0/XIV_Proxy_1.3.1

# ls
redhat-lsb-core-4.0-7.el6.x86_64.rpm
xivproxy-installer-rpm-1.3.1-b612.rhel6.x86_64.bin
xivproxy-installer-rpm-1.3.1.1-b1518.rhel6.x86_64.bin

# ./xivproxy-installer-rpm-1.3.1.1-b1518.rhel6.x86_64.bin
Starting installer, please wait...
International License Agreement for Non-Warranted Programs

Part 1 - General Terms

BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, CLICKING ON AN "ACCEPT"
BUTTON, OR OTHERWISE USING THE PROGRAM, LICENSEE AGREES TO THE TERMS OF THIS
AGREEMENT. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF LICENSEE, YOU
REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND LICENSEE TO THESE
TERMS. IF YOU DO NOT AGREE TO THESE TERMS,

* DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, CLICK ON AN "ACCEPT" BUTTON, OR USE
THE PROGRAM; AND

* PROMPTLY RETURN THE UNUSED MEDIA AND DOCUMENTATION TO THE PARTY FROM WHOM IT
WAS OBTAINED FOR A REFUND OF THE AMOUNT PAID. IF THE PROGRAM WAS DOWNLOADED,
DESTROY ALL COPIES OF THE PROGRAM.

. . . . .
Press Enter to continue viewing the license agreement, or, Enter "1" to accept
the agreement, "2" to decline it or "99" to go back to the previous screen,
```

```
"3" Print.
```

```
1
```

```
Installation completed successfully.
```

```
# rpm -qa|egrep "lsb|xiv"
redhat-lsb-core-4.0-7.el6.x86_64
xivproxy-1.3.1.1-b1518.x86_64
```

10.2.3 Configure and Start XRSC Proxy

The following (bolded) configuration changes should now be made in the /etc/xiv/proxy.conf file. In the changes shown below, "eth0" represents the interface that is being configured for the proxy listener. If multiple interfaces are being used on the Linux Management server, the specific IP address can be entered instead of the eth number.

```
# vi /etc/xiv/proxy.conf
# Configuration file for XIV remote support proxy 1.2

# Mandatory configuration

# Network interface and port that the XIV system will connect to
ListenInterface eth0           (uncomment line and enter IP Address or eth#)
ListenPort 25000               (uncomment line and put port 25000)

# Optional configuration

# Network interface (lo for local) for status queries
# StatusInterface ?
# StatusPort ?

# HTTP proxy for connecting to the Internet
HTTPProxyHost webproxy.wlb2.nam.nsroot.net (uncomment line and enter Web Proxy)
HTTPProxyPort 8080             (uncomment line and enter 8080)
# Optional authentication data for HTTP proxy
# HTTPProxyUser ?
# HTTPProxyPassword ?

# External logger (default is none)
# Logger /usr/share/xiv/syslog-logger

# Restricted user
# User nobody

# Log file
LogFile /var/log/xivproxy.log    (uncomment this line)
```

Once the above changes are completed, the xivproxy should be started and the status should be checked using the following commands.

```
# /etc/init.d/xivproxy status
IBM XIV remote support proxy not running

# /etc/init.d/xivproxy start
Starting IBM XIV remote support proxy:                [ OK ]

# /etc/init.d/xivproxy status
IBM XIV remote support proxy running
```

After it is validated that the xivproxy is running, steps must still be taken on the XIV array itself to complete the configuration. [These steps](#) are given later in the configuration section.

10.2.4 Remove Previous XIV CLI (If Necessary)

If the Linux management station is have the CLI updated to a newer version, the old version should be removed first using the following command.

```
# rpm -qa | grep -i xiv
xiv_cli-4.2.2-build_1

# rpm -ev xiv_cli-4.2.2-build_1
```

Note: For this new release of XIV the Linux Management station should be a new build on a VM with more resources to accommodate the addition of ISIS. As a result, removing old software should not be necessary.

10.2.5 Install XIV CLI (XCLI)

To install the XIV XCLI on the Linux Management server use the following commands.

```
# cd /net/stealth/export1/home1.localhost/sw/Linux/xiv_3.0/XIV_CLI_4.3.1

# ls
xivGUI-4.3.1-build1-linux64.bin

# ./xivGUI-4.3.1-build1-linux64.bin
Preparing to install...
Extracting the JRE from the installer archive...
Unpacking the JRE...
Extracting the installation resources from the installer archive...
Configuring the installer for this system's environment...

Choose Locale...
-----

->1- English
  2- æ¥æ¬èª

CHOOSE LOCALE BY NUMBER: 1

You may cancel this installation at any time by typing 'quit'.

PRESS <ENTER> TO CONTINUE: <CR>

Press Enter to continue viewing the license agreement, or enter "1" to
accept the agreement, "2" to decline it, "3" to print it, "4" to read
non-IBM terms, or "99" to go back to the previous screen.: 1

Choose Install Set
-----
```

Please choose the Install Set to be installed by this installer.

- >1- XIV Storage Management GUI Tools
- 2- XCLI

ENTER THE NUMBER FOR THE INSTALL SET, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
: 2 (NOTE: ONLY CLI is installed here)

=====

Choose Install Folder

Where would you like to install?

Default Install Folder: /root/IBM_XIV_Storage_Management_GUI

ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
: /opt/IBM_XIV_Storage_Management_GUI

INSTALL FOLDER IS: /opt/IBM_XIV_Storage_Management_GUI
 IS THIS CORRECT? (Y/N): **y**
 Installing...

10.2.6 Install ISIS

The ISIS software should also be installed on the Linux Management Station. ISIS is used to associate VMWare WebClients to XIV Storage Pools. Install ISIS with the following commands.

```
# cd /net/stealth/export1/home1.localhost/sw/Linux/xiv_3.0/ISIS-1.2.1-720-
x86_64

# ls
ibm_storage_integration_server-1.2.1-720-x86_64.rpm
ibm_storage_integration_server_java_runtime_extension-1.2.0-66-x86_64.rpm
nginx-1.4.1-1.el6ngx.x86_64.rpm
postgresql92-9.2.2-1PGDG.rhel6.x86_64.rpm
postgresql92-contrib-9.2.2-1PGDG.rhel6.x86_64.rpm
postgresql92-libs-9.2.2-1PGDG.rhel6.x86_64.rpm
postgresql92-server-9.2.2-1PGDG.rhel6.x86_64.rpm
uuid-1.6.1-10.el6.x86_64.rpm

# yum install *.rpm --nogpg
soe6products | 1.2 kB 00:00
soe6u4 | 1.2 kB 00:00
Setting up Install Process
. . . . .
--> Finished Dependency Resolution

Dependencies Resolved
. . . . .
Install 9 Package(s)

Total size: 226 M
Total download size: 452 k
Installed size: 228 M
Is this ok [y/N]: y
. . . . .
Installed:
```

```

ibm_storage_integration_server.x86_64 0:1.2.1-720
ibm_storage_integration_server_java_runtime_extension.x86_64 0:1.2.0-66
nginx.x86_64 0:1.4.1-1.el6.ngx
postgresql92.x86_64 0:9.2.2-1PGDG.rhel6
postgresql92-contrib.x86_64 0:9.2.2-1PGDG.rhel6
postgresql92-libs.x86_64 0:9.2.2-1PGDG.rhel6
postgresql92-server.x86_64 0:9.2.2-1PGDG.rhel6
uuid.x86_64 0:1.6.1-10.el6

```

Dependency Installed:

```
libxslt.x86_64 0:1.1.26-2.el6_3.1
```

Complete!

As soon as ISIS installation completes, the password for the *local* ISIS user account should be set to a strong functional ID type password and stored along with other functional ID's for XIV. Set a Citi CISS Functional ID compliant password for the ISIS user with the following commands while logged in as root.

```
# passwd isis
```

Changing password for user isis.

You can now choose the new password.

A valid password should be a mix of upper and lower case letters, digits, and other characters. You can use a 6 character long password with characters from at least 2 of these 4 classes. An upper case letter that begins the password and a digit that ends it do not count towards the number of character classes used, unless `disable_firstupper_lastdigit_check` option is enabled.

Enter new password: **[Enter password here]**

Re-type new password: **[Enter password again]**

passwd: all authentication tokens updated successfully.

10.2.7 Configure LDAP for ISIS

Once installed, the ISIS application should be configured to use LDAP authentication for the Regional XIV_Admin AD group. At this point in the process the administrator should su to the isis user or login as the isis user and do the following.

Note: When the next commands are run, they should be run with the appropriate LDAP/AD values.

```
# su - isis
```

```
[isis@gdsexiv02 ~]$ cd /opt/ibm/ibm_storage_integration_server/bin
```

```

[isis@gdsexiv02 bin]$ ./isis_ldap configure -e -u "namdev\srv_ibm_xiv"
-s "ldaps://namdev002.namdev.nsrootdev.net:636" -t "ACTIVE_DIRECTORY" -
r "dc=namdev,dc=nsrootdev,dc=net" -g "dc=namdev,dc=nsrootdev,dc=net" -n

```

```
"CN=per_csbe_ibm_xivadmins,OU=Dept_Grps,OU=StorageEng,DC=namdev,DC=nsrootdev,DC=net"
```

Please enter the BIND_DN password (password not shown): **[Enter LDAP Bind ID password here]**

The following changes were applied to the LDAP configuration:
 BIND_DN, SERVER_URI, USER_SEARCH_DN, GROUP_SEARCH_DN, SERVER_TYPE, AUTHENTICATION_GROUP_DN
 Please restart the IBM Storage Integration Server to apply the new configuration..

After the above isis_ldap command is run, it will make the /opt/ibm/ibm_storage_integration_server/conf.d/ldap.ini file will have the following regional LDAP values in it.

```
[isis@gdsexiv02 conf.d]$ cat /opt/ibm/ibm_storage_integration_server/conf.d/ldap.ini

[settings]
enable_ldap = True
server_uri = ldaps://namdev002.namdev.nsrootdev.net:636
user_search_dn = dc=namdev,dc=nsrootdev,dc=net
user_search_key =
group_search_dn = dc=namdev,dc=nsrootdev,dc=net
group_object_class =
authentication_group_dn =
CN=per_csbe_ibm_xivadmins,OU=Dept_Grps,OU=StorageEng,DC=namdev,DC=nsrootdev,DC=net
bind_dn = namdev\srvc_ibm_xiv
bind_password = bnlxb3ZtaWphcnJubmhmbgPt39ZCbHLQkBYoI2kJtog=
bind_pwd_verification =
enpjC2ZtbGZreHBieHRLaYZh3ML6rgShT3IxP1c79S0Z5iHu3CECm71xuAdZLHVP1oqnBa+dIjhouPXWmXL91lsmw8a/T9XBHJYtK71uwXs=
server_type = ACTIVE_DIRECTORY
```

Once the ldap.ini file has the correct values in it, the LDAP SSL certificate needs to be configured into the ISIS LDAP config. The following commands will have to be completed as the root user.

```
# vi /etc/openldap/ldap.conf

# Add the following line at the end of the file and save it.
TLS_CACERT /etc/openldap/certs/xiv_LDAP.pem
```

After the above config file change is made, the PEM encoding of the LDAP Cert should be cut and pasted into a new file named /etc/openlap/certs/xiv_LDAP.pem.

Note: See [LDAP Configuration](#) Section of this document for instructions on how to get the PEM encoding of the LDAP Cert and how to paste it into the file.

```
# vi /etc/openldap/certs/xiv_LDAP.pem
-----BEGIN CERTIFICATE-----
MIIDejCCAu0GAWIBAgIERLgHAZANBgqhkiG9w0BAQUFADAfMQswCQYDVQQGEwJV
UzEQMA4GA1UEChMHV0FSIDE10TAeFw0wNjA3MTQyMDM1MTBaFw0yNjA3MTQyMTA1
MTBaMB8xCzAJBgNVBAYTAlVTMRAdGyDVQQKEwdXQVIGMTU5MIGfMA0GCSqGSIb3
DQEBAQUAA4GNADCBiQKBgQCTKcPCTpoDqN9dr0/MCQtsPG3awk0cTaKd28Sfcz5L
1eYzGN+E8mMOC+YM4/yq+hjwlnVqj09QTYLRYLyG7zd0uYwaHDdhg+V8yG+4ue4T
cP2egmVS3+o49SeF865kvjeKsOne44IldK3M50GAnph6HuLrkFaUVtLtZVXmo0lb
GwIDAQABo4IBwTCCAb0wRwYDVR0gBEAwPjANBgtghkgBhvlvAwMBADANBgtghkgB
hvlvAwMBBDAOBgxghkgBhvlvAwMBAwEwDgYMYIZIAYb5bWFjAQMCMBEGCWCsAGG
+EIBAQQEAWIABZCBtwYDVR0fBIGvMIGsMDAgNKAypDAwLjELMAkGA1UEBhMCVVMx
EDA0BgNVBAoTB1dBUIAxNTkxDTALBgNVBAMTBENSTDEwcqBwoG6GQ2xkYXA6Ly8x
MC40MC40MS4xNjAvb21XQVIlmJAxNTksYz1VUz9jZXJ0awZpY2F0ZVJldm9jYXRp
b25MaXN0P2Jhc2W6J2h0dHA6Ly8xMC40MC40MS4xNTkvQ29tYmluZWZwZWRDRFAvQ1JM
LmNybdARBgNVHRAEJDAigA8yMDA2MDcxNDIwMzUxMFQBDzIwMjYwNzE0MjEwNTEw
WjALBgNVHQ8EBAMCAQYwHwYDVR0jBBgwFoAUiudow9atzRT4qUK4IU8FFCENyKMw
HQYDVR00BBYEFirnaMPwrc0U+KLCuCFPBRQhDcijMAwGA1UdEwQFMAMBAf8wHQYJ
KoZIHvZ9B0EABBAwDhsIVjcuMT00LjADAgSQMA0GCSqGSIb3DQEBBQUAA4GBAGIa
KpWX3vonpG80K0iSSI6eupduVR8hLAaizHM/Pon7ICiY2WnAVHHLpqc/1GMSiKNO
OFVMrVW92xDrnZqR84H0J1VEXNvNI328YlmWf5BNi94TmtQjtDqizpuCW1jcQVg1
o1IiyUETNDHB0QsX6BH7dIiwuJy6Wt1/DLF9Sky3
-----END CERTIFICATE-----
```

As the root user, restart the ISIS agents with the following command.

```
# /etc/init.d/ibm_storage_integration_server restart
Stopping Django service ... [OK]
Stopping celery services ... [OK]
Stopping ds8k proxy.....[OK]
Starting ds8k proxy.....[OK]
Starting celery services ... [OK]
Starting Django service ... [OK]
```

Now as the “isis” user the LDAP configuration should be tested with the following command to validate the configuration is good and working. A test user from the regional xiv_admins AD group should be used for the test.

```
# su - isis
[isis@gdsexiv02 ~]$ isis_ldap test --test_user st49663
Please enter the test user password (or press Enter to skip the
user/password test): [Enter AD password here]

IBM Storage Integration Server LDAP configuration has been verified
successfully.
```

Note: At this point the Linux Management Station VM is completely installed and configured for use. The next section only shows how each user logging in to use the CLI should setup a protected CLI.

10.2.8 Configure CLI Protect

Note: This is NOT a required step at this point in the installation/configuration process for the Linux Management Station nor is it a required step for the root user. Each AD user can follow these steps as they login for the first time.

Each user should log into the Linux Management Station using their own SOE ID and setup the CLI so that no clear text passwords are passed on the command line. First, the `/opt/IBM_XIV_Storage_Management_GUI` directory should be added to the path variable in the users `.bashrc` file. Go to the end of the `~/.bashrc` file and add the following line.

```
[st49663@gdsexiv02 ~]$ vi .bashrc

# User specific aliases and functions
export PATH=$PATH:/opt/IBM_XIV_Storage_Management_GUI

# Now execute the change to the profile
$ [st49663@gdsexiv02 ~]$ . .bash_profile
```

Next, the userid used with the `--protect` option should be the Storage Operations Read-Only Services FID. If a user needs to run admin commands through the CLI they can enter their own user information with the `--protect` options, but should set them back to the [Read-Only services FID](#) when completed.

```
$ [st49663@gdsexiv02 ~]$ xcli --protect
User name: namdev_san_view
Password:
Confirm password:
Credentials saved locally.
```

10.2.8.1 Test CLI

After the certificate has been trusted and the CLI protect options have been setup, the user should test and validate that the CLI is working as it should with the following test.

```
[st49663@gdsexiv02 ~]$ xcli -m 10.40.53.41 version_get
Version
11.4.2.a
```

11. Configuration

All initial configuration of the XIV array is completed by the IBM Site Support Rep (SSR) who does the physical installation. The IBM SSR [uses information gathered during the TDA process](#) to setup the IP management ports, initial event destinations, and rules for getting XIV events back to a monitoring IBM facility. After IBM completes the initial configuration of the XIV, a Storage Administrator only needs to load the GUI or XCLI management interface and start completing specific Citigroup configuration steps discussed in the next sections of the this document.

11.1 Initial ISIS Configuration

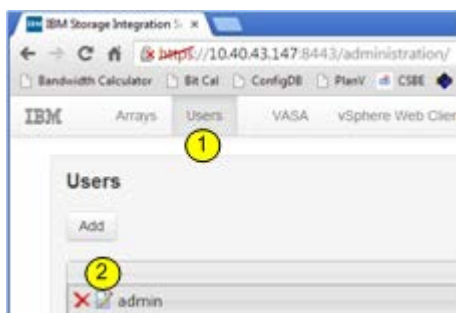
After [ISIS is installed and configured](#) on the Linux Management Station VM there are initial steps that have to be taken to start connecting VMWare WebClients to the XIV storage pools. The following sections will describe how to change the initial admin password, and add XIV arrays and VMWare WebClients into ISIS.

11.1.1 Change Initial admin password

The default admin password should be changed as soon as the ISIS application is accessible in the browser. To complete this task first go to ISIS on a Chrome web browser using the following URL:

[https://\[IP address of Linux Management Server holding ISIS\]:8443/login/](https://[IP address of Linux Management Server holding ISIS]:8443/login/).

Login to ISIS using the admin account using the default password of “*adminadmin*”. Once logged in click on the “Users” tab and hover over the admin user and select the “*Edit*” icon.

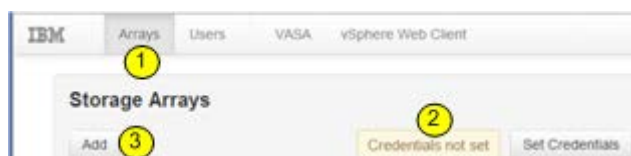


When the next screen appears enter the current password followed by the new password.

Note: The password that is given should comply with all CISS guidelines for functional accounts.

11.1.2 Adding XIV Arrays to ISIS

All arrays in the datacenter where the ISIS server resides should be added into ISIS so that they can give pools to the VMWare clusters via the WebClient. To add an array to ISIS, the array credentials must first be setup. At the main ISIS screen click on the “Arrays” tab and then click on the “Set Credentials” button.



The Set Credentials screen will appear. At this point the administrator should use the [VMWare Plug-In FID](#) named **vmwplugin**. The checkbox stating that this is an directory (AD) account should also be checked.



Once the credentials are set using the vmwplugin account, the arrays can now be added to ISIS by hitting the “Add” button at the previous screen. On the Array screen (not shown) select the *XIV Radial* button and enter one of the Management IP addresses of the array to be added.

11.1.3 Add VMWare WebClients to ISIS

After the XIV Arrays are added to ISIS, the VMWare WebClients should then be added. The process for doing this is very similar to adding arrays. To add WebClients Select the “vSphere Web Client” tab and then hit the “Add” button.

When the *Add vCenter Server* screen appears, enter the name or IP address of the WebClient to be added. In the Username field, the administrator should enter the agreed upon [VMWare "xivisis" FID that has the required "XIV Storage" VMWare role](#) assigned to it. Once saved, the newly added VMWare WebClient will show up in the list back at the main “vSphere Web Client” screen.

11.1.4 Giving WebClients Access to XIV Pools

After VMWare WebClients and XIV arrays have been added to ISIS, Pools must be given to each WebClient so that VMWare Operations can create and provision LUNs to the pools.

From the “vSphere Web Clients” tab in ISIS, the administrator should first highlight the WebClient that the pool will be given to. Once highlighted, the administrator should then hit the “Attach” button on the right side of the screen and the following window will appear.



The administrator should first pick the XIV Array from the drop-down menu and then put a check in the checkbox of the pool on that array that should be attached the WebClient. Once the “Attach” button is hit, the display will return to the WebClient screen and show the association between the WebClient and pool.

11.2 Initial XIV admin Password Change

The default admin password should be changed shortly after the IBM SSR turns the XIV array over to Storage Operations. To complete this task from the man GUI screen select the “View” tab and then “Access->Users” and then expand the “Ungrouped” users. Then right click on the admin user and select “Change Password”. A new pop-up window will appear and allow the Storage Administrator to change the default password for the admin user. The password that is given should comply with all SAA guidelines for functional accounts.

11.3 Change SNMP Community Strings

By default the SNMP community and SNMP trap community strings are set as XIV. These community strings should be set to a value with at least the same strength of a Citigroup compliant password. From the main GUI screen hit the “Systems” tab and then select “System Settings->System”. On the Pop-Up screen that appears hit the “SNMP” tab and change both the SNMP Community and Trap Community values.

To change the default SNMP community strings using the CLI the following commands can be run from the command line or added to a command file:

```
config_set name=snmp_community value="C1t1Gr0up"
config_set name=snmp_trap_community value="C1t1Gr0up"
```

11.4 LDAP Configuration

Due to the lack of acceptable security supplied by standalone means, all non functional ID users will be authenticated using LDAP and Active Directory. Prior to configuring LDAP on XIV, the Citigroup LDAP certificate should be saved in PEM format on the XIV Windows manager server. Go to the following URL: <https://digitalcertificate7.citigroup.com/cda-cgi/clientcgi?action=start>

Near the bottom of this page click on the icon to display the certificate used for LDAP in PEM Encoding format.



The output displayed after this option is selected is the PEM Encoding. Cut from the -----BEGIN CERTIFICATE----- statement to the -----END CERTIFICATE----- statement (with no extra spaces or lines) and save it to a text file named xiv.LDAP.pem on the Management Station. Once the certificate is saved LDAP is ready to be configured. To configure LDAP from the GUI first select the “LDAP Wizard” icon from the “Users” tab main screen.

The following Wizard screen will appear and each tabs required entries will be shown below.



1 - On the *Server Type* Tab set the following:
Server Type: Microsoft Active Directory

2 – On the *LDAP Servers* Tab select the define LDAP server icon which appears as “+”



When the *Define LDAP Server* screen appears enter the following:
FQDN: [enter name of regional server. **ex: NAMDCSW020.nam.nsroot.net**]
Server Address: [enter IP of FQDN server. **ex: 169.185.220.57**]

Note: In the last field called “Certificate File”, browse to and select the pem encoded certificate file that was retrieved in the first step of this process.

Certificate File: [Location PEM was Saved]\xiv.LDAP.pem
Search DN: DC=nam,DC=nsroot,DC=net (**substitute regional values**)

Note: Since XIV LDAP is hard coded, 2-3 Regional LDAP servers should be defined for each GUI. The LDAP servers should reside in the datacenter where the XIV arrays are if possible. At this point the above process should be repeated until (3) LDAP servers are added in the configuration

3 – On the *XIV Users* Tab enter the following:

Service User DM: ***nam_srvc_storage*** (substitute regional values for LDAP FID account. NAM values shown in the example)

Password: ***enter password of [LDAP bind user/FID](#)***

Confirm Password: ***enter password of LDAP bind user again***

4 – On the *Unique ID's* Tab enter the following:

User ID Attribute: ***sAMAccountName***

User Name Attribute: ***sAMAccountName***

XIV Group Attribute: ***memberOf***

5 – On the *Groups* Tab enter the following:

Storage Admin Role:

CN=SAN_Support,OU=Misc_Grps,OU=CPNA,OU=CS,DC=nam,DC=nsroot,DC=net (substitute regional values. NAM values shown in the example)

Security Admin Role:

CN=SAN_Security,OU=Misc_Grps,OU=CPNA,OU=CS,DC=nam,DC=nsroot,DC=net

Note: Until the Known Issue surrounding the Security Administrator role Discussed in the [Release Notes Known Issues](#) section is resolved, this group should be created and the XIV should be pointed at it, ***but no users should be added to it.***

Read Only Role:

CN=SAN_View,OU=Dept_Grps,OU=SolanaDC,OU=SYS,DC=nam,DC=nsroot,DC=net (substitute regional values. NAM values shown in the example)

6 – On the *Secure LDAP* enter the following:

Use SSL: ***Yes***

First Warning: ***60***

Second Warning: ***30***

Third Warning: ***14***

7 – On the *Bind & Cache* Tab leave all values at the default levels.

8 – On the *Test & Activation* Tab enter the following:

Use LDAP: ***Yes***

Put a check in the Test LDAP Configuration checkbox

User Name: **Enter an LDAP user tied to an AD group**

Password: **Enter the password for the above account**

9 – On the *Finish* Tab just hit the finish button.

11.5 XIV XRSC Support Center Definition

XRSC is used for Vendor Remote Support and there are two separate parts that require configuration. The XRSC proxy [installation](#) and configuration is completed on the [Linux Management Station when it is installed](#).

Once the XRSC proxy has been [configured and started](#) the XIV Array has to be pointed at it. From the main GUI screen select *Tools > Support Center*. When the following screen appears hit the “add support center” icon which appears as “+”. Leave the Port Type pull-down menu set to Management as shown below.



Once the support center screen appears the fields should be populated with the proxy server information.

1. Enter a name for the connection at the local datacenter. Enter in the format of Citi_<datacenter>_XRSC-#.
2. In the Address field enter the IP address of the Linux proxy server that was configured.
3. In the port field enter the port used in the proxy configuration (25000).
4. In the priority field enter the highest number of the total number to be defined. (if 5 will be configured then 5 would be the priority of the first)
5. Hit the Define button.

Note: The first XRSC proxy server should be defined and have its priority set to 2, then a second one from the remote datacenter should also be defined and have its priority set to 1.

Once at least two XRSC proxy servers are defined, go back to the support center screen and at this point a connection can be attempted by selecting the “*Connect Support Center*” icon.

Once the connect support center screen appears it should be populated with the following *minimum* values depending on the work IBM is doing. Set the Session Timeout to 10800 (3 Hours) and then set the Idle Timeout field to 7200 (2 Hour). Enter a standard Citigroup XIV password in the Connection Password field.¹⁵

Note: The XRSC password is a one-time temporary password used only to access the SSL connection. Once validated the IBM support person would still have to authenticate at the XIV array via functional ID.

¹⁵ A temporary one time password can be used for opening XRSC connections. The password should be strong and given to the IBM Tech needing to use the open connection.

Note: When IBM asks for an open XRSC connection they should be asked how long they will need it and the appropriate timeout value should be set and they should be informed that the idle timeout will be set to two hours. The administrator should also give IBM the temporary XRSC one-time password.

The same configuration shown above can be completed using the following CLI commands.

```
XIV-7820031>>support_center_define support_center="Warren_Lab11-1"
address=10.40.42.90 port=25000 priority=2
XIV-7820031>>support_center_define support_center="Warren_Lab11-2"
address=10.40.42.91 port=25000 priority=1

XIV-7820031>>support_center_list
Name          Address      Port    Priority
Warren_Lab11-1 10.40.42.90 25000   2
Warren_Lab11-2 10.40.42.91 25000   1

XIV-7820031>>support_center_connect timeout=180:00 idle_timeout=120:00
password=CitiXIV123
Command executed successfully.
```

Once the connection is made it will show up as idle until an IBM remote call-center technician connects to it. To validate the connection is up and running waiting for a connection use the following CLI command.

```
XIV-7820031>>support_center_status
State    Connected sessions   Timeout (min)   Module          Connected
since    Destination
idle     0                    87.1           1:Module:1      2012-02-02
17:12:56 Warren_Lab11-1 (10.40.42.90:25000)
```

If an IBM remote call-center technician connects it will show up in the XIV event log as shown below. A "REMOTE_SUPPORT_CONNECT" event will be displayed followed by any commands executed by the "xiv_maintenance" or "technician" user as shown below.

2012-01-13 12:47:12	REMOTE_SUPPORT_DISCONNECT		System disconnected from ...	XIV-7820031
2012-01-13 12:39:27	VOLUME_CREATE	xiv_maintenance	Volume was created with na...	XIV-7820031
2012-01-13 12:38:50	CUSTOM_EVENT	xiv_maintenance	test xrsc	XIV-7820031
2012-01-13 12:27:55	REMOTE_SUPPORT_CONNECT		System connected to remot...	XIV-7820031

Connections to the XIV will also be shown in the /var/log/xivproxy.log file on the xiv proxy server that was configured. These logged connections will show

```
Jan-13 12:27:51 Info New connection from 10.40.53.81:53767
Jan-13 12:27:51 Info Connection established 10.40.53.81:53767 <> (HTTP
proxy: 192.193.171.216:8080) <> 195.110.41.142:443
Jan-13 12:27:52 Info SSL connection with 195.110.41.142:443 using
AES256-SHA (256 bits)
Jan-13 12:47:11 Info Connection closed 10.40.53.81:53767 <> (HTTP
proxy: 192.193.171.216:8080) <> 195.110.41.142:443
```

11.6 Pool Creation

Although the production XIV arrays have 243TB (base 10) usable space, A single large **Regular** pool should be created using all the space. Since all over-provisioning will be maintained at the VMWare level and snapshots are not part of this certification, the single pool should be created as a *regular pool* while allocating 0 space for snapshots. Pools can be created in the GUI or using the following xcli command.

```
pool_create pool="0281_3TBSATA" size=243392 lock_behavior=read_only
snapshot_size=0
```

The naming convention for the pool should be **[XIV serial number]_DriveType**

11.7 Host/Cluster Creation on XIV

To create hosts from the GUI go to the main “Hosts and Clusters Screen” and select the “Add Hosts” icon. The following screen will appear where the host name, cluster, and type will need to be entered. All host types except HP-UX should be set to default.

After the host is created the HBA ports will need to be added to the host definition. Highlight the host that was just created and right click on it and select “Add Port” and the following screen will appear where the HBA WWPNs can be

selected for the host. The host must be zoned to the XIV in order for the ports to show up in the pull down menu.

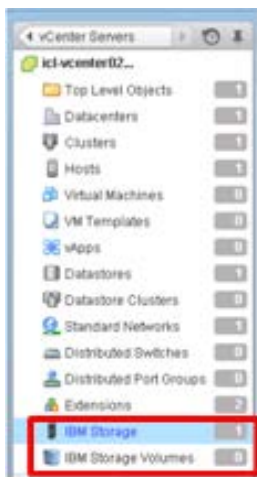


The above process will have to be completed for each zoned HBA. Below is a CLI example of adding a host along with its HBAs.

```
XIV-7820031>>host_define host="sangs22"
XIV-7820031>>special_type_set host="sangs22" type=default
XIV-7820031>>host_add_port host="sangs22" fcaddress="10000000C939254A"
XIV-7820031>>host_add_port host="sangs22" fcaddress="10000000C93AD1EE"
```

11.8 LUN Creation on XIV using vCenter WebClient Plug-in

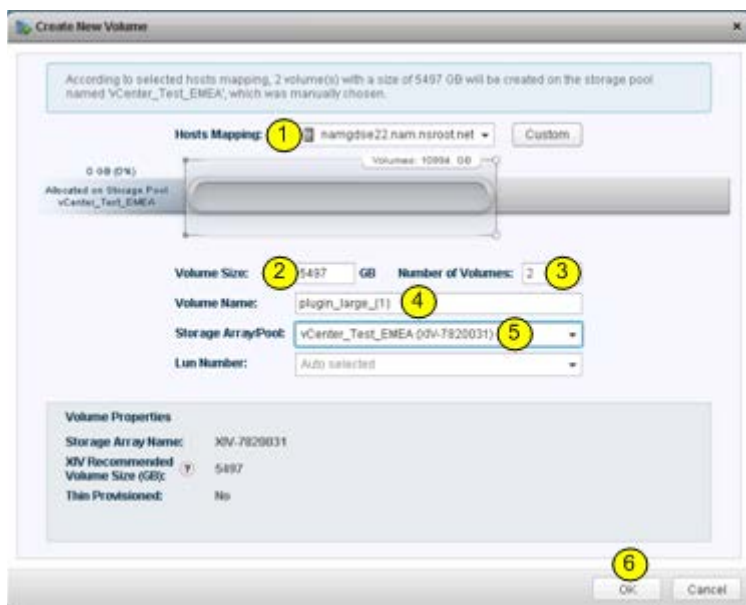
Provisioning of LUNs by the VMWare administrators will be done through the IBM Storage vCenter WebClient plug-in. In order for provisioning to occur, The VMWare Cluster should have already been zoned to the XIV, an [XIV array](#) and the specific [WebClient](#) should have already been added to ISIS, and a [pool should have be attached to the WebClient](#) in ISIS. Both the Array and the array volumes should show up under the appropriate vCenter servers.



To provision new LUNs, first click on the “IBM Storage” item under the vCenter server where the specific XIV is located. Then click on the specific XIV and “right click” on the array and select “Create New Volume” as shown below.



The following screen for creating new volumes will appear.



1. Pick the specific node/cluster to provision the LUNs to
2. Enter the size of either a small or large Standard VMWare LUN.

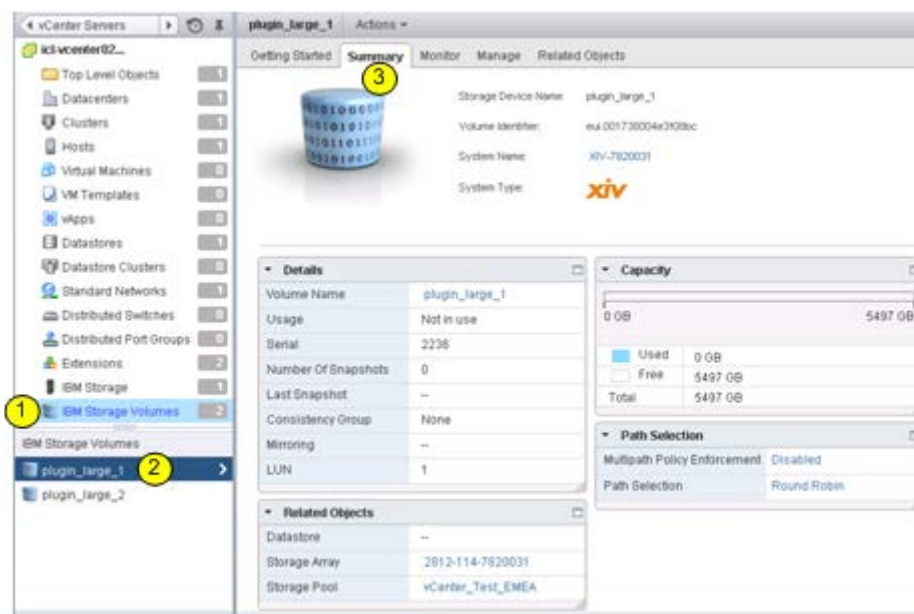
Note: When creating volumes through the vCenter plug-in base 10 sizes are used. The values for the (2) standard VMWare LUN sizes that should be used on this screen are: 1 – Small LUN 1.4TB (**1546 GB** base 10) and 2 – Large LUN 5TB (**5497 GB** base 10). See [LUN Sizing for vCenter Plug-in](#) section of this document for further detail.

3. Enter the Number of LUNs to create.
4. Enter the name of the volume. If creating multiple volumes leave the “_1” in the name field as it will number the LUNs.

Note: Naming convention for the VMWare LUN names should use the following format: XIV_[VMWareClusterName]_ (do not leave trailing underscore out).

5. Select the desired pool from the drop-down menu.
6. Hit the “OK” Button and the LUNs will be created.

Once the LUNs have been created they can be viewed in detail on the screen of the particular cluster that they were assigned to as shown below.



1. Select the “*IBM Storage Volumes*” resource under the vCenter server where the volumes were created.
2. Select the specific LUN to look at.
3. Click the “*Summary*” tab.

For more detailed information on using the XIV WebClient plug-in refer to Chapter 5 of the ISIS users Guide at the following URL: [ISIS Users Guide](#)

11.9 Event Notification

In order to have SNMP events sent to the Citigroup Tivoli infrastructure or a Storage Operations SAN Support DL, the following items must be completed.

- [Create a event destinations](#) (Tivoli and DL)
- [Create event rules](#) (Tivoli and DL)
- [Validate Aperture Fields](#) (Tivoli Only)
- [Validate IP in SMRWEB](#) (Tivoli Only)

Note: for a complete list of the Critical events that will be handled by Tivoli please refer to [Appendix “A”](#).

11.9.1 Creating a Tivoli or SAN Support DL Destination

To define an event destination for Tivoli or a SAN Support DL, select the “View” tab from the main GUI screen of the appropriate XIV and then select “Monitor > Events” and then select the “Rules” icon.

When the Rules screen appears, select the “Destinations” tab on the left side and then select the add destinations icon (a “+” on the GUI). A drop-down menu will appear and *Destination* should be selected.



When the *Define Destinations* screen appears enter the following for each field:

Destination Type: SNMP (for Tivoli) or EMAIL (for SAN Support DL's)

Destination Name: TIV1 or TIV2 (for Tivoli) or **San Support** (For SAN Support DL)

IP/DNS: Regional Tivoli server IP Address (for SNMP destinations)

If this is an EMAIL destination these extra fields will have to be filled out also:

Existing User: None

Email Address: The actual email address of the SAN Support DL

Gateways: All

The Tivoli SNMP and SAN Support DL EMAIL destinations can also be created using the following command lines.

Note: For the TIVOLI and SEMS two destinations should be created for each rule and then a destination group should be created (shown below in CLI).

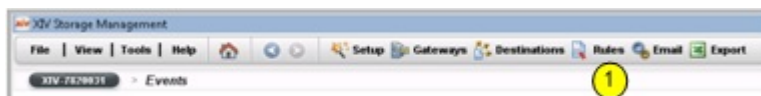
```
XIV-7820031>>dest_define type=SNMP dest="TIV1"
snmp_manager=192.168.184.138
XIV-7820031>>dest_define type=SNMP dest="TIV2"
snmp_manager=192.168.188.145
XIV-7820031>>destgroup_create destgroup="TIVOLI"
XIV-7820031>>destgroup_add_dest destgroup="TIVOLI" dest="TIV1"
XIV-7820031>>destgroup_add_dest destgroup="TIVOLI" dest="TIV2"

# To Define a SAN Support DL destination the use the following:
```

```
XIV-7820031>> dest_define type=EMAIL dest="San Support"
email_address="dl.cti.nam.mwdc.ibm.san.alert@imcnam.ssmb.com"
smtpgws="all"
```

11.9.2 Creating Tivoli or SAN Support DL Rules

Once the Tivoli and SAN Support destinations have been defined, rules must now be created for the events. This can be completed in the GUI or from the CLI. To create rules using the GUI select the *Rules* icon from the main event screen.



When the *Rules* screen appears select the “Rules” tab on the left and then select the add rule icon (a “+” on the GUI). When the “Create Rules” screen appears (shown below) enter the following for each field:

Rule Name: Tivoli (for Tivoli) or SAN Support (for SAN Support DL)

Min Severity: Major (for both Tivoli and SAN Support DL)

Event Code: All

Destinations: TIVOLI (Tivoli destination group) or SAN Support (for SAN Support DL)



The CLI commands that could be used to create the Tivoli and SAN Support DL rules are shown below.

```
XIV-7820031>>rule_create rule="TIVOLI" min_severity=Major codes=All
dests="TIVOLI" snooze_time=0
```

For the SAN Support DL rule use the following:

```
XIV-7820031>>rule_create rule="San Support Alerts" min_severity=Major
codes=All dests="San Support" snooze_time=0
```

Note: In the above example the dest=TIVOLI is a destination group that is made up of two destinations (TIV1 and TIV2)

11.9.3 Validate Aperture Fields

For Tivoli alerting to work correctly the following fields must be defined in Aperture and have the correct values. The example given below is for NAM and other regions should substitute their regional values.

When new XIV arrays come into the datacenter the Global Enterprise Hardware Planning team will create an Aperture entry for each array. It is imperative that each region give them this list of fields and their required values for XIV arrays.

Note: In the table below North America values are shown. These values are region specific

Aperture Field	NAM Values for XIV
Business Area	Citigroup Technical Infrastructure
Machine Category	Production
Device Type	SAN Attached storage
Machine Type	Storage Sub-System
Database Type	N/A
Platform	Vendor Specific (PC)
Backup Type	N/A
Device Availability Monitoring	Tivoli - NA
Device Availability Monitoring Tier	SNMP Pass-Through
Application ID	149141
Application Name	NA SAN Infrastructure
Support Group type	System Support Group
Support Group Name	NA Storage Management
Primary Contact	Doug Novellano
Secondary Contact	Douglas Chin
Problem Management Method	Virtual Tech
Problem Management Queue Name	cti-na-san-support

Once Aperture data has replicated, log into SMRWEB at the following URL: <https://smrweb.nam.nsroot.net> and ensure that the information for each XIV has replicated. This can be validated by performing a “search” operation on device name.

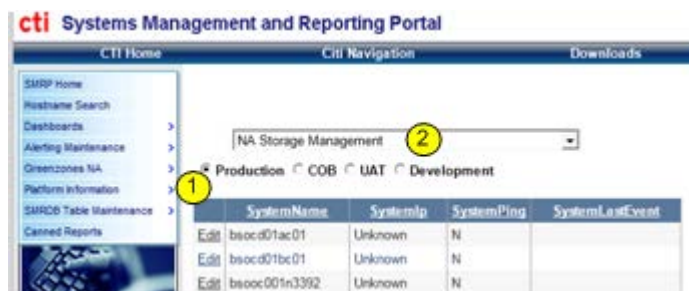
11.9.4 Validate Correct XIV IP in SMRWEB

Login to SMRWEB at the following URL: <https://smrweb.nam.nsroot.net> and validate that the XIV has correct IP address defined. To update the device IP,

select “SMRDB Table Maintenance -> SNMP IP and No Ping Maintenance” from the menus on the left side of the page as shown below.



The following screen will appear. First select the *Production* radial button and then select the *appropriate region* from the pull-down menu.



Then select the *Edit* button of the XIV name and update the IP address. After the update select the *Y* hyperlink to test.



11.9.5 Adding New Events to Tivoli Include List

Over time it may be necessary to add more events to the list of events that Tivoli will page out on. To accomplish the Administrator should first open a CMP request for **Global Data Center Operations Automations Request** at this URL: https://cmp.nj.smb.com/marketplace/control/product/~productId=47307_253071_GLOBAL#

On the Request enter the values for the associated specific fields.

- Appropriate Service Offering: **Tivoli ITM 6 Monitoring**
- Choose Tivoli Operations: **Add/Delete/Modify Tivoli Host**
- Select Tivoli Host Action: **Modify Tivoli Host**
- Monitor Type: **App Support**
- Download the Monitoring Specification: **At this point upload a text file that contains the new event to have added to the XIV_Rules file on Tivoli**
- Description of Modification: **Put a brief description saying the new event (NAME THE EVENT) needs to be added to the XIV_rules**

11.10 Chargeback and Capacity Reporting

Currently XIV is only approved and certified for VMWare LVM environments. As a result, ALL chargeback reporting is now being handled by the VMWare operations team. If it is decided that the XIV would be certified for general storage, it would have to be integrated into the Storage Operations chargeback infrastructure. Future chargeback reporting may be done with EMC SRM which is currently being certified.

11.11 Performance Reporting

The normal XIV GUI will keep 30 days of granular data and up to a year of non granular performance data that can be referenced. However, to store granular data for more than 30 days the XIV performance reporting software can be installed on at least one Windows management station. After the [XIV reporting software installation](#) the following steps should be taken to configure it for operation.

It should first be validated that “[Install_Path]\XIV_Perf_0.18\xpvyv” is in the system PATH variable. Next an xml config file will need to be created in the [Install_Path]\XIV_Perf_0.18 directory that uses the following format.

Note: In the config file below the “interval=10” represents the minute interval to pull stats and the “count=144” is the number of times to pull that interval. The example config file below is pulling 144 counts of a 10 minute from an array (10 minute intervals for the last 24 hours). To set the config to pull a week worth of data at 20 minute intervals, the interval would be 20 and count would be 504

```
- <root>
- <report name="Daily_Perf_Report" type="performance" interval="10"
count="144" output_format="csv" folder="C:/tmp/perf_output"
auto_name_sub_folder="yes">
  <system_id name="xiv_0274" />
  <system_id name="xiv_0275" />
  <system_id name="xiv_0281" />
```

```
# First change to the Performance Reporting directory
C:\ cd [Install_Location]\XIV_Perf_0.18

# Now encrypt the config file created in the previous step
[Install_Location]\XIV_Perf_0.18> xpyv xiv_reporter.py -c
config_file.xml -e

# Now delete the previous config file with the clear text password
[Install_Location]\XIV_Perf_0.18> del
config_file.20##.##.## ##.##.##.xml
```

11.12 SANscreen Integration

To discover the XIV in SANSscreen the following items must be completed.

- Regional SAN Screen team must install the TPM XIV Management package CITI_WIN_XIVGUI_431_00 on the regional SANSscreen server where the XIV will be discovered.
- The Storage Operations team should give the SANSscreen team the [read-only services FID account](#) and password for accessing the XIV.

- The Storage Operations team should validate that TCP port 7778 is opened through the CEP to and from the Regional SANscreen server.
- The SANscreen team should then discover one of the XIV management IP address on the SANscreen console.

Note: SANscreen reports all LUN mapping numbers as XIV blocks converted to Base 2 and all array capacity numbers as XIV Base 10 numbers converted to Base 2.

11.13 Log Review and Reconciliation (SEMS)

Currently the XIV array does not support syslog for forwarding of log files to a centralized location for log review and reconciliation. However, CSBE worked with the SEMS team and they have setup an SNMP trap receiver for the XIV to send all log entries to for log review and reconciliation. In order to send log entries to the SEMS SNMP trap receiver the following items should be completed.

- Setup a production and COB SEMS destination using the GUI, or by using the following CLI command

```
XIV-7820031>>dest_define type=SNMP dest="SEMS1"
snmp_manager=169.185.236.228
XIV-7820031>>dest_define type=SNMP dest="SEMS2"
snmp_manager=169.173.44.17

XIV-7820031>> destgroup_create destgroup="SEMS"
XIV-7820031>> destgroup_add_dest destgroup="SEMS" dest="SEMS1"
XIV-7820031>> destgroup_add_dest destgroup="SEMS" dest="SEMS2"
```

- Setup a SEMS rule using the above destination via the GUI or by using the following CLI command.

```
XIV-7820031>>rule_create rule="SEMS" min_severity=none codes=All
dests="SEMS" snooze_time=0
```

Note: In the above SEMS rule the dest=SEMS is a destination group that is made up of two destinations (SEMS1 and SEMS2)

The SEMS team has been given and XIV include list of events to do reconciliation upon. The *include list* contains events that are generated as a result of user/administrator tasks on the XIV array. Although every attempt was made to find every user generated event, they list may need minor updates as new versions of microcode come out.

11.14 EMC SRM Integration

EMC Storage Resource Management (SRM) will be used for XIV Data Collection. Unlike other products that collect data from XIV that require the XIV CLI be loaded on the collecting servers, SRM uses the CIM port. In order for EMC SRM to be setup and configured the Storage Operations team should work with the SRM team to make sure the following items are completed.

- The (3) XIV Management Port IP Addresses for each XIV array in the region should be given to the SRM team.
- The [XIV Read-only Services FID](#) and password should be given to the SRM team.
- A [Firewall rule](#) for each regional SRM XIV Collector should be opened to the CIM ports (5988, 5989) for each XIV.

Once the above steps have been taken it should then be validated the each SRM XIV collected is able to retrieve all the necessary data from the XIV arrays.

Note: If SRM fails to discover or poll the XIV it may be that the CIM service needs to be started on the XIV. See the [Release Notes document Known Issues](#) section for more details about this issue.

11.15 HP Network Automation (HPNA) Integrations

HPNA is an automated tool for validating that each XIV has all values set in accordance with the Standard Build Configuration Checklist (SBCC). In order for this to occur a few items must be pre-configured.

- The HPNA Linux servers that will monitor the XIV Arrays will have to [load the XIV CLI](#) on each of the servers.
- The (3) XIV Management Port IP Addresses for each XIV array in the region should be given to the HPNA team.
- The [XIV Read-only Services FID](#) and password should be given to the HPNA team.
- Any regional specific settings (Ex: LDAP Server, Mail-hubs. Etc.) for each region should be given to the HPNA team so that a regional policy can be configured for all XIV's in the region.
- A [Firewall rule](#) for each HPNA server should be opened to port 7778 for each XIV.

Once all the above steps have been taken, the HPNA team will configure the HPNA servers to routinely check the XIV configuration.

11.15.1 Setup HPNA Destination Groups (Tivoli and SEMs)

As part of the new XIV configuration for HPNA, each region should setup destination groups for both Tivoli and SEMs. The currently defined destinations for both Tivoli and SEMs should be added to the new destination groups using the GUI or following CLI commands.

```
XIV-7820031>> destgroup_create destgroup="SEMS"
XIV-7820031>> destgroup_add_dest destgroup="SEMS" dest="SEMS1"
XIV-7820031>> destgroup_add_dest destgroup="SEMS" dest="SEMS2"

XIV-7820031>> destgroup_create destgroup="TIVOLI"
XIV-7820031>> destgroup_add_dest destgroup="TIVOLI" dest="TIV1"
XIV-7820031>> destgroup_add_dest destgroup="TIVOLI" dest="TIV2"
```

Note: If the current Tivoli and SEMs destinations do not have the standard names of TIV1, TIV2, SEMS1, and SMES2, then they should be renamed to these names. Failure to do so will result in an XIV violation on the HPNA tracking report.

Note: After the new TIVOLI and SEMS destination groups have been created, the TIVOLI and SEMS rules with have to be update to use the new destination groups instead of the individual destinations. Also, If the Tivoli and SEMS rules do not have the name of TIVOLI or SEMS the names should be changed to this when the rule is updated to use the destination groups. Failure to do either of these will result in an XIV violation on the HPNA tracking report.

12. Best Practices

The following CATE Storage best practices should be followed for the XIV Gen 3 Storage arrays. These recommendations are in accordance with all compliance findings and have been discussed with both internal Storage Operations/Integration team and the IBM vendor.

12.1 Array Over-Subscription

The XIV arrays are capable of doing over-commitment provided the commands are issued by the IBM maintenance user and an IBM RPQ has been signed. However, since the XIV arrays are currently only used by VMWare LVM environments at Citigroup, all over-commitment will be maintained at the ESX layer using Storage DRS (similar to the VNX file design). Over-commitment of the Array would have to be revisited if the XIV get certified for general storage use.

12.2 Storage Pool Creation

Since the XIV Array only has a single RAID and disk type, pools are only used as an organizational tool as opposed to a QOS type separator. As a result of the XIV architecture, it will be considered a CSBE best practice, to create one pool containing all capacity which will result in much easier scripts and line commands that will be used as it pertains to chargeback and capacity reporting. The single large pool should be an XIV regular pool with no snapshot space reserved which can then be connected to by multiple ESX clusters.

12.3 Pool Threshold Alerting

Once a pool reaches its hard limit the storage pools will go into read only mode and no changes can be made to any LUNs in that pool until the hard limit is increased or existing data is moved to another location. Pool threshold alerting will let storage administrators know when a pool is reaching a hard limit. The following initial best practice thresholds will be used for alerting on pool usage: Warning 85%, Minor 90%, Major 95%, and Critical 98%.

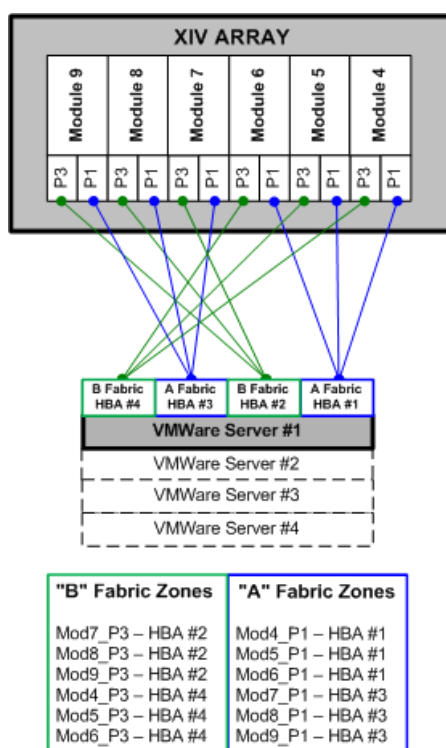
12.4 Pool Locking

If a pool reaches its hard limit there are two possible ways the pool can react as it pertains to continued server I/O requests. The pool can be configured as “Read-Only” or “No I/O”. It will be considered a CSBE best practice to set any pool to a “Read Only” locking behavior.

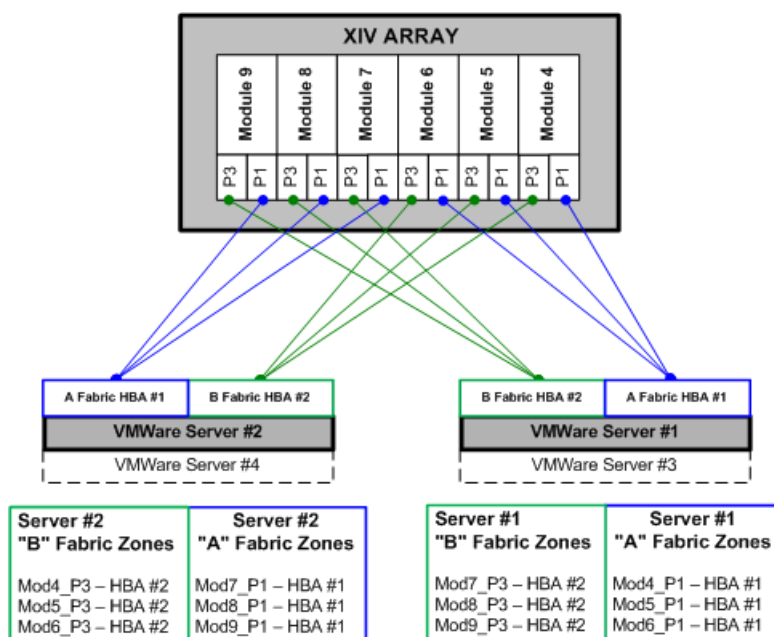
12.5 VMWare Zoning

The IBM best practice zoning for XIV is to have every server HBA zoned to every XIV I/O module port on the same fabric. This best practice is recommended to all I/O spread evenly across each grid component (in this case I/O modules). Due to ESX path limitations of 1024 total paths per server/node, this IBM recommended best practice will not be used. The zoning best practice will be to have each ESX *node* zoned to each I/O module instead of each I/O module port. To get the desired balance across the I/O modules it will require that each ESX node HBA be zoned to (3) I/O module ports (3:1 ratio) as shown in the following diagrams.

12.5.1 Zoning With 4 HBA Ports Per ESX Server



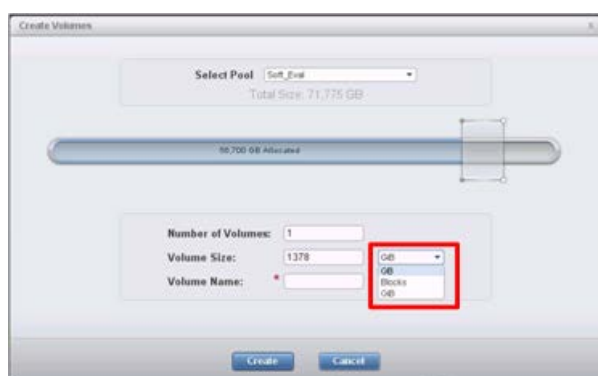
12.5.2 Zoning With 2 HBA Ports Per ESX Server



12.6 LUN Creation

12.6.1 Decimal (Base 10), Binary (Base 2), and Block Options

On the XIV there are three different options when creating LUNs. In the GUI these types show up as GB, GiB, and Block as shown below on the LUN creation screen.



The default option for creating LUNs (volumes) on XIV is GB. It is important to note that the GB represents GB in Decimal (base 10), not Binary (base 2). GiB represents GB in Binary (base 2) or 1024 bytes. Blocks are represented as 512 KB blocks.

12.6.2 XIV Rule of 17 GB

The physical capacity associated with a logical volume on XIV is always a multiple of 17 GB (base 10) because the volume spans all physical drives in the array due to the grid nature of the architecture. Therefore, while it is possible to present a block-designated logical volume to a host that is not a multiple of 17 GB, the actual physical space that is allocated on the XIV for the volume will always be a number of 17 GB increments needed to meet the block-designated capacity.

As a result of the XIV Rule 17GB, any attempt to create a volume (LUN) on the XIV GUI using GB (decimal) or GiB (binary) will automatically be rounded up to the nearest 17 GB increment.

12.7 LUN Sizing

The XIV storage system distributes data across all disk drives – for each allocated volume. In general, to yield better performance with XIV it is best to allocate fewer volumes with larger sizes. Using minimum number of volumes needed for data separation and keeping the volume sizes bigger will allow XIV to better utilize cache algorithms such as pre-fetch and LRU (least recently used).

12.7.1 LUN Sizing using vCenter WebClient Plug-in

Standard XIV LUN Type	Matching LUN Type	Base 10 Size Entered in vCenter Plug-in (GB)	Base 2 Capacity Size shown in vCenter Plug-in (GiB)	Base 10 Size shown on vCenter Plug-in	Size Shown in SANscreen
1.4 TB VMWare Standard Small	EMC 1.40 TB VMWare	1546 GB	1442 GiB	1548 GB	1442.37 GB
5 TB VMWare Standard Large	N/A	5497 GB	5128 GiB	5506 GB	5128.44 GB

NOTE: When creating LUNs in the vCenter WebClient plug-in, there is no option to create LUNs in Base 2 (GiB). If for any reason LUNs need to be created using blocks it will have to be completed by the Storage Administrators using the XIV GUI.

12.7.2 Data Migrations

The XIV array based migration tools nor replication will be certified for use with VMWare LVM environments. All required migrations should be completed using VMWare Storage vMotion.

12.8 ISIS Application

The ISIS application will be the layer that VMWare will use to get any polling information from XIV arrays, and all information that relates to the associating of XIV pools to vSphere WebClients. The following best practices should be followed when deploying ISIS.

- ISIS should be deployed on one [Linux Management Station VM](#) in each major datacenter in a region
- Any desktop that plans to manage ISIS Storage functions should do so using [Google Chrome](#)
- ISIS should always be configured to use LDAP and pointed at the regional XIV Admins AD group. The local admin account should have the password changed upon installation and only be used as a functional ID in the event of an LDAP/AD failure
- VMWare WebClients should only be put on a single ISIS server
- XIV Arrays should only be put on a single ISIS server
- VMWare WebClients and XIV arrays that are NOT in a major datacenter can be added to ISIS across the network. *This should be done only as an exception.*
- Any datacenter that ends up having two or more XIV arrays should then be considered a major datacenter and have a [Linux Management Station VM](#) put in place. Any XIV array or WebClient should then be migrated over to the new ISIS server in the local datacenter

12.9 LUN Naming

XIV LUNs can be named in any convention that makes sense to the administrator. However, if LUNs are created at the time of provisioning it may be helpful in performance views if the LUN name contains the ESX cluster name that it is provisioned to. For all ESX environments the LUN name should also have XIV_ at the beginning of the name so the administrators will know they are responsible for the over-commitment of the LUNs. The naming convention that should be used for all VMWare environments should follow this convention:

XIV_[ESXClusterName]_LUN#

12.10 Remote Vendor Support

For vendor remote support, the IBM XRSC product was certified for the XIV Array. An XRSC proxy/gateway will be configured and running on the [Linux Management Station](#) that will provide a secure SSL connection through the Citigroup web proxy server, that will only allow connections to and from (2) IBM remote call center IP addresses. This connection which is initiated by Citigroup administrators can also be password protected provided the IBM account

manager for Citigroup has been informed of the password that the call centers would use.

Although the XRSC connection is configurable to never timeout, it is an SAA requirement that a timeout is set each time a connection is opened to the remote IBM call centers.

Note: An XRSC connection to IBM should always be password protected at all times with the XRSC SSL temporary one-time password.

12.11 Host Attached Kits (HAK)

Host Attached Kits (HAKs) are a small collection of tools used in the support and installation/configuration of hosts attaching to the XIV array. All storage vendors have these type kits or tools that usually include at the very least a LUN inquiry command and some type of grab command. Normally CSBE pulls the inquiry and grab commands out of these packages and includes them in the CSBE SANinfo package.

Currently for VMWare environments there is no HAK and as a result they will not be part of this certification.

12.12 VAAI Driver Support

The IBM Storage Device Driver for VMware VAAI is a software plug-in that is integrated with the VMware ESX 4.X environments, as part of VMware's vStorage APIs for Array Integration (VAAI). The IBM software plug-in consists of a kernel module that reports to the VMware VAAI driver and allows offloading extended VMware operations to supported IBM storage systems.

The following extended VMware operations can be offloaded to the supported IBM storage systems:

- Full copy (clone) – Copies data from one logical unit (LUN based) to another without writing to the ESX server. Rather than issuing read and write requests from the host, the data copying operation is initiated on the storage system. This speeds up the virtual machine (VM) cloning operation and reduces the CPU load on the host.
- Block zeroing – Assigns zeroes to large storage areas without actually sending the zeros to the storage system. This speeds up the VM initiation operation, and reduces the I/O and CPU load on the host.
- Hardware-assisted locking – Locks a particular range of blocks in a shared logical unit, providing exclusive access to these blocks. Instead of using SCSI reservation that locks the entire logical unit, locking specific blocks is a more efficient alternative that greatly improves scalability in large server

arrays. The locking is performed using Atomic Test & Set (ATS) commands.

With ESX 5.X the driver is now an in-box driver and as such no external packages are required to be loaded to take advantage of the above functionality.

12.13 IBM XIV Plug-in for VMWare vSphere WebClients

Together with supported IBM storage systems that are managed by ISIS (IBM Storage Integration Server), the deployed IBM Storage Enhancements (WebClient Plug-in) enable the following management features on vSphere Web Client side for registered vCenter servers:

- Full control over storage volumes, including volume creation, resizing, renaming, migration to a different storage pool, mapping, unmapping, multipath policy enforcement, and deletion.
- Easy and integrated allocation of volumes to VMware datastores, used by virtual machines that run on ESX and ESXi hosts, clusters, or datacenters.

Note: The IBM Storage Enhancements are automatically deployed and made available for the [vCenter WebClients/Servers that were registered \(added\) in ISIS](#).

12.14 Host Multi-Pathing Options

Currently it is the IBM best practice to use MPIO for host multi-pathing when attaching to XIV arrays, although Veritas DMP is also a supported multi-pathing option. Since the XIV arrays are only certified for VMWare LVM environments in Citigroup, native multi-pathing will be used at the ESX layer. All pools managed through the vCenter WebClient plug-in should be set to round robin multi-pathing.

12.15 Provisioning

All LUNs should be created and mapped through the vCenter WebClient plug-in. The LUNs default to round-robin when they are created and mapped. [Standard LUN naming](#) and [LUN sizes](#) should be used for all provisioning.

12.16 De-Provisioning

Any time a server has its LUNs unmapped from an XIV array, those LUNs should be completely deleted so that all data on the LUNs is destroyed. This also releases the LUNs storage space back to the array free pool and assures that the LUN complete with all of its data, is not given to another server or cluster node.

12.17 LDAP Role Mapping

On previous microcode version for the XIV, it only supported two LDAP roles used for accessing the array. These roles are administrator and read-only and both could have only ONE corresponding AD group defined. The read-only role is used for running reports and the admin role is used by the administrators for the initial configuration of the array, and making all LDAP changes.

With this new release of microcode, multiple groups can now be pointed at a single XIV role and a new Security Role has been added. However, both of these new pieces of functionality have known issues that are discussed in the [Release Notes document](#).

Until these known issues are resolved, each XIV role should continue to be pointed at just a single AD group, and although an AD group needs to be created for the new Security Administrator role, NO users should be added to the group.

12.18 XIV Cross-Domain LDAP Authentication

AD Cross-Domain authentication used for Follow-The-Sun support has never been certified for XIV in Citigroup. For this new release of the XIV it was tested and it does work. However, there were multiple issues found associated with approving it for production with this release.

Specifically, CSBE could only get it to work using Universal Nested groups while Citigroup AD Engineering only supports “Domain Local” nested groups. It was also found that once cross-site authentication was configured on the XIV, that the ISIS application could no longer add arrays to the configuration because ISIS did not understand nested groups. See the Known Issues section of the [Release Notes document](#) for more detailed information.

Until these known Issues are resolved, Follow-The-Sun support cannot be certified and this would have to be accomplished by adding an account in each AD domain for each Follow-The-Sun support user.

12.19 IBM RAID Configuration (RAID-X)

The RAID configuration is one of the areas that make the XIV storage array unique from most other arrays. In most arrays there are several different RAID types and disk types used.

XIV has taken a different approach to RAID. Due to bigger disks, RAID systems are taking longer to recover from a failed disk. Traditional RAID systems recover a disk by reading all the remaining disks in a RAID group beginning to end and

by writing the missing data beginning to end to an online spare disk. Taking longer to recover a failed and replaced disk is a risk in two ways.

First, it means that the period of vulnerability (the time it takes to replace a failed disk and recover its contents) is getting longer as drive sizes increase. During this time, more failures can lead to data loss or a longer period of vulnerability.

Second, recovery is a lot of work. It reduces disk accesses for users, lowering the disk performance for user workloads. The longer the recovery, the longer the periods in which users are possibly impacted.

The XIV is a grid-based storage system that does not use traditional RAID. Instead, The XIV divides each LUN into 1MB chunks, and stores two copies of each chunk on separate drives in separate modules. Although this is similar to RAID-10, IBM calls this RAID-X. It is also important to note that the 1MB chunks are spread across every drive in the entire array.

When a failure occurs, the system knows exactly which partitions are no longer protected and immediately begins creating new copies to restore redundancy. This is where the parallelism of the design comes into play. The entire machine works to re-create the missing redundancy, so very little work has to be done by any one component. This allows XIV to rebuild a failed 2 TB drives in about an hour as opposed to the time it would take in traditional RAID implementations.

12.20 Wrap Executables

The wrap executables were used to cover clear text passwords on the CLI command line. Now that IBM has delivered the `--protect` functionality with XCLI, the wrap executables will no longer be needed for running normal commands from the CLI and can be removed from the Management Station.

However, for administrators running large script command files (Like shown in Appendix A) that want to be prompted for passwords (ex: LDAP bind ID) the wrap executable can be kept on the system and used for this purpose.

The wrap executable is used to run CLI command files from the Windows or Linux SOE management stations. This version of the wrap command will conceal clear text passwords by prompting the user for the passwords where the `%_PASSWORD_PASSWORD_%` variable shows up in the command file. The wrap executable should not be used for any batch programs that will require command line passwords as it will prompt for them. The wrap executable works best for any interactive CLI commands that require passwords.

Once the wrap package is installed, command files can be created and run with the following syntax from the Management stations instead of the XIV array CLI

(meaning the output and information can be stored and displayed on the management station instead of standard out on the CLI).

(Command file example)

```
# vi xiv_coms
version_get
config_get
support_center_connect password=%_PASSWORD_PASSWORD_%
```

(Linux example)

```
# ./xiv_wrap_linux64 -y -m 10.40.53.81 -u admin -r xiv_coms
```

(Windows example)

```
# C:\tmp>xiv_wrap.exe -y -m 10.40.53.81 -u admin -r xiv_coms.txt
```

Enter password: (Enter XIV Admin password here)

**support_center_connect password=%_PASSWORD_PASSWORD_%Enter password:
(Enter password for XRSC connection here)**

Version

11.1.0.a

Name	Value
dns_primary	10.40.32.11
dns_secondary	
system_name	XIV-7820031
snmp_location	Unknown
snmp_contact	Unknown
snmp_community	XIV
snmp_trap_community	XIV
system_id	20031
machine_type	2812
machine_model	114
machine_serial_number	7820031

email_sender_address

email_reply_to_address

email_subject_format {severity}: {description}

iscsi_name iqn.2005-10.com.xivstorage:020031

ntp_server 10.40.32.11

support_center_port_type Management

isns_server

ipv6_state disabled

Command executed successfully.

Note: When using the wrap executable the password should not be given (-p option) in the command file because the wrap command will prompt if it is not there. The wrap command will also prompt for any variable passwords in the command file that show up in the form of %_PASSWORD_PASSWORD_%.

13. Operational Procedures

13.1 Backing up ISIS Configuration

With this first release of ISIS there is no built-in clustering and as a result the Linux Management Station that holds ISIS will be on a VM to help redundancy. Along with the current lack of clustering the backup and restore process is also still evolving. For this first release of ISIS, the backup process has had several RFE's (*Request For Enhancements*) turned into IBM to refine the process.

In order to backup ISIS there should first be a small network mount location to hold the backup files, or they can be stored locally but would have to be recovered from tape before ISIS could be recovered. The ISIS backup should be performed any time there is a change to the ISIS configuration. Use the following steps to backup the ISIS configuration.

Note: The ISIS backup process ONLY backs up the XIV Arrays, VMWare WebClients, and Pool associations, and both XIV and VMWare credentials that have been put in ISIS. It currently does not backup any other parts of ISIS like the LDAP configuration.

- While logged in as the **isis** user validate that the local directory or mount point that will hold the backup files is owned by the isis user.

```
[isis@gdsexiv02 ~]$ ls -ld /mnt/isis_backup
drwxr-xr-x 2 isis isis 4096 Jun  9 08:49 /mnt/isis_backup
```

NOTE: In this example a network mount is being used for the backups.

- Now run the backup command outputting the file to the backup directory location. The backup file requires a 16 char key that we will automate using the Unix date command as shown below.

(Backup Command Syntax)

```
# isis_configuration backup -f <file name> -k <16 character key>
```

(Now run the backup command)

```
[isis@gdsexiv02 ~]$ isis_configuration backup -f
/mnt/isis_backup/`uname -n`_isis_backup.`date +%H%M%d%Y%Y` -k `date
+%H%M%d%Y%Y`
```

The configuration of IBM Storage Enhancements for VMware vSphere Web Client has been backed up successfully.
Backing up the configuration to the file
/mnt/isis_backup/gdsexiv02_isis_backup.1426062020142014.conf completed successfully.
The backup operation has been completed successfully.

(Now validate that the backup was completed)

```
[isis@gdsexiv02 ~]$ ls -l /mnt/isis_backup
total 4
-rw-rw-r-- 1 isis isis 745 Jun 20 14:26
gdsexiv02_isis_backup.1426062020142014.conf
```

At this point ISIS has a backup of all the XIV Arrays, XIV Array credentials, VMWare WebClients, and all pool associations.

13.2 Restoring ISIS Configuration

If ISIS needs to be restored, it can be done with the commands shown below. However, prior to the restore command being run, ISIS needs to be completely removed and a clean install and configuration must be done. Prior to doing a restore the Storage Administrator should take the following steps.

- Remove ISIS and do a [clean install of ISIS](#).
- [Configure LDAP for ISIS](#)

Once the above steps have been taken, issue the following command to restore all of the Array, Array Credentials, WebClients, and Pool Associations, information in ISIS.

(Restore Command Syntax)

```
# isis_configuration restore -f <file name> -k <16 character key>
```

(Now run the backup command)

```
[isis@gdsexiv02 ~]$ isis_configuration restore -f
/mnt/isis_backup/gdsexiv02_isis_backup.1426062020142014.conf -k
1426062020142014
```

```
Reading Config File: gdsexiv02_isis_backup.1426062020142014.conf
Storage credentials have been set successfully.
IBM storage array XIV-7820031 has been added successfully.
Import of VASA admin users has been completed successfully.
vCenter server connection parameters have been added successfully.
attach pool vCenter_Test_EMEA of array 2812-114-7820031 to vcenter
969B8FB1-AFD9-41BC-A876-E19FEE481E1C
Pool vCenter_Test_EMEA has been successfully attached to vCenter server
969B8FB1-AFD9-41BC-A876-E19FEE481E1C.
The configuration of IBM Storage Enhancements for VMware vSphere Web
Client has been restored successfully.
Configuration restore from the specified file has been completed
successfully.
```

Note: After a restore has completed, the [array credentials](#) in ISIS will need to be changed from local back to directory because of a known issue. Without taking this step, no new arrays can be added to ISIS. See the [Release Notes document Known Issues](#) section for more details about this issue.

13.3 Upgrading from Old vCenter Plug-in to WebClient Plug-in

When the vCenter application is replaced by a new vSphere WebClient, all information stored by the old XIV plug-in about pools associations to VMWare clusters must be transferred to the new ISIS server. At the time of writing of this document, this would have to be a manual process as there is no current way to export the old plug-in information and have it import into ISIS.

In order to do this the following should be completed in the order shown below:

- First identify the vCenter server Clusters that will be migrated over to a WebClient.
- Identify the new ISIS that will hold the XIV array, New WebClient, and pool associations
- Add the XIV Array, WebClient, and pool associations to ISIS, and then validate that the XIV array shows up on the new WebClient
- The old plug-in and information should then be removed on the old vCenter server

14. Security Considerations

After going through the SAA process, the following NCI (Non Compliant Issues) are covered by **RE #502151**. These issues are listed in the SAA NCI document at the following URL: [SAA NCI Document](#), and a GAP resolution along with timeframes is listed in the NCI GAP Resolution plan at the following URL: [NCI GAP Resolution Plan](#) on the **tab marked 3-plan**. As the issues are resolved in future IBM microcode releases they will be removed from this document.

14.1 XRSC Findings

These first set of findings deal with the IBM XRSC (XIV Remote Support Center). XRSC is a proxy/gateway service running on an internal Linux management station that allows a secure SSL connection to be initiated by Citigroup to IBM call centers from the XIV arrays. The XIV array itself will initiate this connection when remote support is required. The secure SSL connection will have a temporary one-time password set on it when the connection is open by Storage Operations.

14.1.1 APP009, APP011, APP013, and APP017 – Password Policy

These (4) findings all deal with the temporary one-time XRSC SSL password (that is not associated with an XIV user) that is used each time a new XRSC connection is opened. This password can be set on the temporary SSL connection that is initiated by Citigroup from the XIV array. Specifically, SAA wants this temporary one-time password for the SSL connection to abide by the Static Password Strength Policy (APP009 - CISS 11.5.3.2), Static Password Aging Policy (APP011 - CISS 11.5.3.4), Static Password History Policy (APP013 - CISS 11.5.3.4.c), and Maximum Failed Login Attempts Policy (APP017 - CISS 11.5.1.1).

Normal logins to the XIV arrays use LDAP authentication and all of these policies are met. However, for this temporary one-time password on the secure SSL connection initiated by Citigroup, policy enforcement is not met just like it is not met on a functional ID. IBM has stated it will not add this functionality to a temporary one-time password that is not associated with a user account. As a result, it will be documented in this solutions guide that these SAA policies be manually applied to any temporary SSL connection password that is initiated.

It may also be decided to drop this extra one-time password (simply extra security) and just open the secure SSL connection without a password. This would close all of the items dealing with this password since it is not required. Without this password on the SSL connection, IBM support would still have to authenticate at the array which does abide by all Citigroup password policies.

Until a further ruling is made by SAA, Storage Operations should only assign temporary passwords to the SSL connection that comply with normal Citigroup password strength policies listed in CISS 11.5.3.2.

14.1.2 APP044 and APP098 – Non EATDS Approved Solution

This finding points out that the IBM XIV XRSC vendor remote support is not Citigroup internal EATDS (Enterprise Architecture Technology Domain Standard) approved. XRSC will likely never be EATDS approved by Citigroup so it may always require an open Risk Acceptance. See CISS section 11.4.2.1 for more details.

Although XRSC is not EATDS approved, the XRSC methodology for remote vendor support has been approved by the Citigroup C3PAR / 3rd Party Working Group and the Global Network Engineering groups. These groups are currently working with SAA to see if they can cover XRSC under EATDS or come up with a new classification for it along with other vendor remote support tools for EMC and HDS that use this same methodology/technology.

14.2 XIV and GUI Findings

14.2.1 CVA 2056 – Low Encryption

This CIVA finding deals with the XIV responding to GUI requests that can be low-grade encryption of less than 128 bits.

IBM claims to have resolved this in the new 11.4.2.a microcode that is included in this certification. A follow-up CIVA Scan is being scheduled for late Q4 2014 to validate that this issue is resolved.

14.2.2 CVA 2055 – SSLv2.0 Access

This CIVA finding deals with the XIV accepting SSL v2.0 clients for access. This finding states that only SSLv3.0 should be allowed.

IBM claims to have resolved this in the new 11.4.2.a microcode that is included in this certification. A follow-up CIVA Scan is being scheduled for late Q4 2014 to validate that this issue is resolved.

15. Appendices

15.1 Appendix “A” – XIV Events sent to Tivoli

Although all MAJOR and CRITICAL events will be sent to both the regional SAN Support DL and Tivoli, only this list of events will be sent to the Tivoli Consoles and page the necessary Storage operations team members to address the issue.

Event Code	IBM Severity Level	Description
HEARTBEAT_EMAIL_HAS_FAILED	minor	Sending heartbeat to Destination Name via SMTP Gateway failed. Module: Module ID ; Error message: 'Error Message'; timeout expired: Timeout Expired?
STORAGE_POOL_EXHAUSTED	major	Pool 'pool' is full. All volumes are locked. Troubleshooting Enlarge Storage Pool or move or delete volumes or Clones with Clone Deletion Priority 0.
STORAGE_POOL_VOLUME_USAGE_TOO_HIGH	major	Usage by volumes of Storage Pool with name 'pool.name' has reached current% of the total pool size. Troubleshooting Increase pool size or decrease snapshot size .
SMTP_GATEWAY_FAILED	major	SMTP gateway with name 'name' has failed. It will not be used until Retry Time.
DATA_LOSS	critical	Manager found data loss in num_lost_slices slices.
EMERGENCY_SHUTDOWN_NOW	critical	System is shutting down in emergency shutdown mode due to: Emergency Shutdown Reason. Troubleshooting Please contact your Administrator.
SHOULD_BE_EMERGENCY_SHUTDOWN	critical	An emergency shutdown has been detected, but UPS control is disabled. Shutdown reason: Shutdown Reason. Troubleshooting Solve the UPS problem immediately or shut the system down using 'shutdown -y' and contact support.
STORAGE_POOL_VOLUME_USAGE_INCREASED	variable	Usage by volumes of Storage Pool with name 'pool.name' has reached current%.
EMAIL_HAS_FAILED	variable	Sending Event Code (Event Index) to Destination List via SMTP Gateway failed. Module: Module ID; Error message: 'Error Message'; timeout expired: Timeout Expired?.


```

ldap_config_set user_id_attr="sAMAccountName"
ldap_config_set user_name_attr="sAMAccountName"
ldap_config_set xiv_group_attr="memberOf"

ldap_config_set
storage_admin_role="CN=SAN_Support,OU=Misc_Grps,OU=CPNA,OU=CS,DC=nam,DC=nsroot,DC=net"

(New Change for This XIV Release)
security_admin_role="CN=SAN_Security,OU=Misc_Grps,OU=CPNA,OU=CS,DC=nam,DC=nsroot,DC=net"

ldap_config_set read_only_role="
CN=SAN_View,OU=App_Grps,OU=SAN,OU=INFRA,DC=nam,DC=nsroot,DC=net"

ldap_config_set xiv_password=%_PASSWORD_PASSWORD_%

ldap_mode_set mode="Active"

(Changed in this Release. See new commands Below)
# Setup Tivoli SNMP Events
(New Change for this XIV Release*****)
dest_define type=SNMP dest="TIV1" snmp_manager=192.168.184.138
dest_define type=SNMP dest="TIV2" snmp_manager=192.168.188.145
destgroup_create destgroup="TIVOLI"
destgroup_add_dest destgroup="TIVOLI" dest="TIV1"
destgroup_add_dest destgroup="TIVOLI" dest="TIV2"
rule_create rule="TIVOLI" min_severity=Major codes=all dests="TIVOLI"
snooze_time=0

# Setup SAN Support SMTP Events
dest_define type=EMAIL dest="San Support"
email_address="dl.cti.nam.mwdc.ibm.san.alert@imcnam.ssmb.com"
smtpgws="all"
rule_create rule="San Support Alerts" min_severity=Major codes=All
dests="San Support" snooze_time=0

(Changed in this Release. See new commands Below)
# Setup SEMS SNMP Events
(New Change for this XIV Release*****)
dest_define type=SNMP dest="SEMS1" snmp_manager=169.185.236.228
dest_define type=SNMP dest="SEMS2" snmp_manager=169.173.44.17
destgroup_create destgroup="SEMS"
destgroup_add_dest destgroup="SEMS" dest="SEMS1"
destgroup_add_dest destgroup="SEMS" dest="SEMS2"
rule_create rule="SEMS" min_severity=none codes=all dests="SEMS"
snooze_time=0

# XRSC Commands - These commands should only be added to the
# configuration script if the XRSC proxies are configured and the
# service is up and running.

support_center_define support_center="Warren_Lab_11_1"
address=10.40.42.90 port=25000 priority=2 support_center_connect
password=%_PASSWORD_PASSWORD_%

```

```

support_center_define support_center="Warren_Lab_11_2"
address=10.40.42.91 port=25000 priority=1 support_center_connect
password=%_PASSWORD_PASSWORD_%

# Create the Storage Pool
pool_create pool="0281_3TBSATA" hard_size=243392 soft_size=243392
lock_behavior=read_only snapshot_size=0

# Set Storage Pool Threshold Alerts
event_redefine_threshold severity=Warning threshold=85
event_redefine_threshold severity=Minor threshold=90
event_redefine_threshold severity=Major threshold=95
event_redefine_threshold severity=Critical threshold=98

```

The above command file can be run on the Windows or Linux Management station using the syntax shown below. The following output assumes that xiv_wrap.exe is in the PATH and that the above commands file was saved as C:\tmp\coms.txt

```

# First set XCLI admin password with --protect option.

C:\Users\Administrator> xcli --protect
User name: admin
Password:
Confirm password:
Credentials saved locally.

# Now run the commands file with the xcli.

C:\Users\Administrator> xcli -m 10.40.53.41 -r C:\tmp\coms.txt
Note: Long output of the above command not shown here

# Set XCLI password back to a read-only account.

C:\Users\Administrator> xcli --protect
User name: st49663_ro
Password:
Confirm password:
Credentials saved locally.

```

15.3 Appendix “C” – Current XIV Specifications

The table below shows the current XIV specifications for functionality certified. This table will be updated with new functionality as it is certified or update with any changes as a result of new microcode.

General Hardware		
1	Number of disks per data module	12
2	Memory per data module	24 GB
Performance		
3	Maximum queue depth per FC host port	1,400
4	Maximum queue depth per mapped volume per [host port, target port, volume]	256
Spare Capacity		
5	Hot spare space allocation	15 Drives (whole module + 3 drives)
Host Mapping		
6	Maximum volumes mapped per host	512
Host Management		
7	Maximum number of clusters	100
8	Maximum number of hosts	1000
9	Maximum number of defined WWNs/iQNs	4000
10	Maximum number of concurrently logged in host ports	350 per port, 700 per interface module, 4,200 per machine
Storage Pools And Volumes		
11	Maximum number of storage pools	256
13	Maximum size of a storage pool	243 TB
14	Minimum size of a volume	17 GB
15	Maximum size of a volume	161 TB
16	Maximum number of volumes + snapshots	12000
Event Handling		
17	Maximum number of gateways (SMTP, SMS)	8
18	Maximum number of destination groups	32
19	Maximum number of destinations (email, SMS, SMTP, SNMP)	100
21	Maximum destinations in rule	32
22	Maximum destinations per event notification rule	32
23	Maximum number of event notification rules	100

16. References

Document	Location
CSBE XIV Generation 3 Home Page	https://catecollaboration.citigroup.net/domains/platstor/gdse/products/techstdshmpgs/XIV.aspx
XIV R11.42 Release Notes	https://catecollaboration.citigroup.net/domains/platstor/gdse/products/platforms/IBM%20XIV/CSBE-14020-RN.pdf
VMWare VSI Storage Design Document	https://catecollaboration.citigroup.net/domains/platstor/gdse/products/Designs/CSBE-11079-DD.pdf
XIV Implementation Guide	https://catecollaboration.citigroup.net/domains/platstor/gdse/products/platforms/IBM%20XIV/XIV_Architecture_Implemetation_Usage.pdf
XIV ISIS Users Guide	https://catecollaboration.citigroup.net/domains/platstor/gdse/products/platforms/IBM%20XIV/IBM_Storage_Integration_Server_1.2.0_UG.pdf
XIV CLI Reference	https://catecollaboration.citigroup.net/domains/platstor/gdse/products/platforms/IBM%20XIV/XIV_CLI_Reference.pdf
XIV XRSC Users Guide	https://catecollaboration.citigroup.net/domains/platstor/gdse/products/platforms/IBM%20XIV/XRSC_1.3.0_UsersGuide.pdf