Dell EMC Metro node 7.0.1

Security Configuration Guide

7.0.1

July 2021

Notes, cautions, and warnings

ⓘ **NOTE:** A NOTE indicates important information that helps you make better use of your product.

△ **CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.**

⚠ **WARNING: A WARNING indicates a potential for property damage, personal injury, or death.**

Contents

1

Metro node overview

Metro node virtualizes the data that is on storage arrays to create dynamic, distributed, and highly available data centers.

Use metro node to:

- Move data non-disruptively between Dell EMC storage arrays and non-Dell EMC storage arrays without any downtime for the host.

  Metro node moves data transparently, and the virtual volumes retain the same identities and the same access points to the host. There is no need to reconfigure the host.

- Protect data in the event of disasters or failure of components in your data centers.

  With metro node, you can withstand failures of storage arrays, cluster components, an entire site failure, or loss of communication between sites (when two clusters are deployed) and still keep applications and data online and available.

With metro node, you can transform the delivery of IT to a flexible, efficient, reliable, and resilient service.

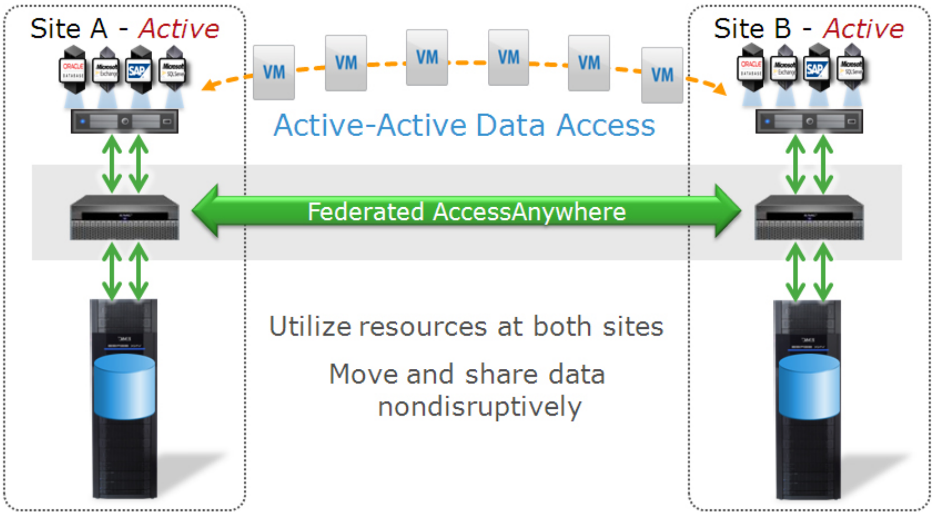
Site A - Active
Site B - Active
VM
Active-Active Data Access
Federated AccessAnywhere
Utilize resources at both sites
Move and share data nondisruptively

Figure 1. Metro node active-active

Metro node addresses these two primary IT needs:

- **Mobility**: Metro node moves applications and data between different storage installations:
  - Within the same data center or across a campus (metro node Local)
  - Within a geographical region (metro node Metro)
- **Availability:** Metro node creates high-availability storage infrastructure across these same varied geographies with unmatched resiliency.

Metro node offers the following unique innovations and advantages:

- Metro node distributed/federated virtual storage enables new models of application and Data Mobility.

  Metro node is optimized for virtual server platforms (VMware ESX, Hyper-V, Oracle Virtual Machine, AIX VIOS).

  Metro node can streamline or accelerate transparent workload relocation over distances, including moving virtual machines.

- In a Metro configuration, metro node AccessAnywhere provides image consistent active-active access to data across two metro node clusters.

Metro node pools the storage resources in multiple data centers so that the data can be accessed anywhere. With metro node, you can:

- Provide continuous availability and workload mobility.

- Replace your tedious data movement and technology refresh processes with metro node’s patented simple, frictionless two-way data exchange between locations.
- Create an active-active configuration for the active use of resources at both sites.
- Provide instant access to data between data centers. metro node allows simple, frictionless two-way data exchange between locations.
- Combine metro node with virtual servers to enable private and hybrid cloud computing.

2

Security recommendations

While the Security Configuration Guide must be reviewed in its entirety, this segment serves to check most important security recommendations of Dell EMC to ensure the security of your data and environment.

⚠ **WARNING: iDRAC passwords are auto-generated. Manually updating the iDRAC password is not supported, and can impact product functionality or cause data unavailability.**

- Given the elevated permissions that are granted to the service account, its password must be changed to better protect metro node from misuse or abuse of those privileges. Service account password and iDRAC root password are changed automatically during initial system configuration.
- Given the elevated permissions that are granted to the iDRAC root account, its password must be changed to better protect metro node from misuse or abuse of those privileges. Use the command `vplex_system_config --idrac` to change the password.

  ⓘ **NOTE:** For more information, see Appy iDRAC in the *Dell Storage Systems Configuration and Installation Guide for Metro Node Appliance* on SolVe.
- To retrieve the auto-generated password, run `/opt/dell/vplex/system_config/bin/system_config_collect.py --SHOW-IDRAC-PWD`.

Security configuration settings

This section provides an overview of user accounts and privileges.

Topics:

- User roles, accounts, and privileges

User roles, accounts, and privileges

Table 1. Metro node user accounts and privileges

Component	Account Type	Default password	Privileges
Metro node	**service**	-	● Access to the metro node management server desktop, VPlexcli, and Unisphere for metro node UI. ● Run permissions for VPlexcli related scripts. ● Ability to run VPlexcli commands. ● Read/write access to log files. ● Ability to run the System Configuration commands.
	admin	`teS6nAX2` (1)	● Access to metro node management server desktop, VPlexcli, and Unisphere for metro node UI. ● Ability to create, modify, and delete new user accounts. ● Ability to run VPlexcli commands. ● Read-only access to log files.
	Metro node user (default user)	null	● Access dependent on that granted with Role-based User Access. See Role-based User Access for complete descriptions of user types and permissions.
Metro node iDRAC	root	calvin	● Root privileges ● Access to the metro node desktop. ● The default password is removed during the System Configuration process. ⓘ **NOTE:** The iDRAC passwords are set using metro node, and they meet the Dell security requirements. Connecting the iDRAC port to the customer network is not supported. The iDRAC must be accessed only using Customer Support over Metro node. ⚠ **WARNING: iDRAC passwords are auto-generated. Manually updating the iDRAC password is not supported, and can impact product functionality or cause data unavailability.**

1. The first user who attempts to log in as admin is prompted to change the admin password before logging in.

2. Given the elevated permissions that are granted to the service account, its password must be changed in order to better protect metro node from misuse or abuse of those privileges. Changing the service account password provides more information.

ⓘ **NOTE:** The default policies can be modified using `vplex_system_config` command. For more information, see *Configuration and Installation Guide for the Metro node appliance* available in Solve.

Configuring user authentication

Metro node customers can choose to configure their user accounts using either:

- An external OpenLDAP or Active Directory server which integrates with UNIX using Service for UNIX 3.5, Identity Management for UNIX, or other authentication service.

  OpenLDAP and Active Directory users are authenticated by the server. Usernames and passwords that are created on an external server are fetched from the remote system to the metro node system each time they are used.

- The metro node management server

  Usernames and passwords are created locally on metro node system, and are stored on metro node.

Customers who do not want to use an external LDAP server for maintaining user accounts create their user accounts on the metro node system itself.

Metro node is pre-configured with two default user accounts: admin and service.

See the *Dell EMC CLI Guide for metro node* for information about the commands used to configure user authentication.

Topics:

Role-based access control feature overview

To improve security, shell access is limited to the **admin** and **service** users only.

See the *CLI Reference Guide for metro node* for more information about the `User add` command with the `-r` option.

Users who are defined as either **admin** and **service** will be taken to the shell command line once logged-in to the metro node management server. Users not having shell access are redirected to the Vplexcli.

All users using LDAP credentials are defined as **`vplexuser`** by default.

Individual login credentials can be set for LDAP users as every user account has a different username and password. However, all LDAP users are given identical privileges (same role and same shell access value). The Administrator can either grant or revoke shell access to any customizable role, such as **`vplexuser`**.

Connecting to the metro node management server (Local and Metro), Logging on to metro node CLI (Local and Metro),

The user automatically logs in to the CLI (unless that user is **admin** or **service** or is defined as having shell privileges by the Administrator).

NOTE: In order to issue shell commands, you must either be logged in as **admin** or **service** or have shell access that is explicitly granted by the Administrator.

SCP file transfers

Metro node allows file transfer to/from the metro node management server using SCP. SCP permissions are granted with shell access.

Users with no shell access can perform SCP on files only (not on directories) from or to a single directory. An additional CLI context represents this SCP directory.

ⓘ **NOTE:** If you do not have shell access, you can only access a single directory when uploading and downloading files.

LDAP/AD user authentication

For the metro node access to LDAP/AD users, see the **Authenticate Service Directory** document available in SolVe. The LDAP document on SolVe can be found under **Admin** > **Configure**.

5

Manage passwords and Password policy

Topics:

Change password

Use `vplex_system_config` command to change service and admin password.

Password policy

The system is supplied with default password policy which is not changeable.

6

Log file settings

This section describes log files relevant to security.

Log file location

Table lists the name and location of metro node component log files relevant to security.

Table 2. Metro node component log files

Component	Location
Unisphere for metro node	/var/log/VPlex/cli/session.log_*username*
Software management server	/var/log/messages
Firewall	/var/log/firewall

Log file management and retrieval

All logs rotate automatically, to avoid unbounded consumption of disk space.

Communication security settings

This section describes the communication security settings that enable you to establish secure communication channels between metro node components, as well as metro node components and external systems.

Topics:

IP WAN COM

A metro node Metro system does not support native encryption over an IP WAN-COM link. It is recommended that you deploy an external encryption solution such as IPSec to achieve data confidentiality and end point authentication over IP WAN COM links between clusters.

Th metro node uses the TCP protocol for its IP WAN-COM communications. Configure TCP ports on the firewall for IP WAN-COM communications. If the firewall type is filter and not proxy, you must open the following firewall ports:

- TCP ports
  - Port 61484
  - Port 61483
  - Port 61482
  - Ports 32768 to 61000

Ports

The following table lists all the network ports used by Metro node components.

Port Number	Protocol	Service Name	Description
22	TCP	sshd	Used for shell access (bash if service user, vplexcli if other user).
22	TCP	cws: ssh	Cluster witness server ssh port
123	UDP	chronyd	NTP Chronyd
323	UDP	chronyd	NTP Chronyd
323 &123	TCP	cws : NTP	director-1-1-A ip should be provided for the Chrony service. CWS chronyd usage
5020	TCP	iSM	Redirects HTTPS requests to the iDRAC Web GUI. Remote RACADM can support going over this port as well to reach the iDRAC.
61001	UDP	cws:	Cluster Witness Server listens on this UDP port
61482	TCP	nsfw	TCPCOM out
61483	TCP	nsfw	TCPCOM in

Port Number	Protocol	Service Name	Description
61484	TCP	nsfw	TCPCOM cx