



# What's New in VMware Cloud on AWS Version 1.24

VMware Architecture

## Table of contents

What's New in VMware Cloud on AWS Version 1.24 .....	3
Overview .....	3
Aria Suite .....	4
Network Enhancements .....	5
SDDC Group to Group Connectivity .....	5
NSX Alarms Improvements .....	5
Enhanced IPv6 Support .....	5
vSAN Express Storage Architecture .....	7
External Storage Enhancements .....	8
VPC Peering .....	8
Increased NFS Performance .....	8
VMware Cloud Sizer .....	9
Security Enhancements .....	10
Granular NSX Admin Roles .....	10
New CA and TLS 1.3 Support .....	10
Lifecycle Management Improvements .....	12
Virtual Machine Hardware .....	13

## What's New in VMware Cloud on AWS Version 1.24

### Overview

In this article, we will take a closer look at the newest release of the Software-Defined Data Center (SDDC) version 1.24 for VMware Cloud on AWS which has quite a few security and performance improvements under the hood and introduces new capabilities for the customers.

The SDDC version 1.24, released on the 14th of November 2023, comes with an updated bill of materials and features the most recent versions of vSphere including vCenter and ESXi with vSAN 8 Update 2 and NSX 4.1.2.

SDDC version 1.24 is an essential release meaning that every new SDDC deployed after general availability (GA) will use it. However, existing SDDCs must be upgraded to 1.24 to cater to all features available in the release. This happens according to VMware Cloud on AWS lifecycle management. You can explore details of the lifecycle process in this article [Infrastructure Lifecycle Management Done for You with VMware Cloud on AWS](#).

Certain features are not tight to the release and are accessible for both “greenfield” and “brownfield” customers. Also, certain features are available upon request through VMware representatives in preview mode. We will highlight the bundle dependencies where relevant.

## Aria Suite

The VMware Aria Suite is now part of VMware Cloud on AWS new subscriptions, providing even better cloud management for our customers. The following key VMware Aria enterprise products and capabilities are included:

- VMware Aria Automation: Modern, self-service infrastructure automation to streamline IT processes and deliver a DevOps-ready automation platform.
- VMware Aria Operations: AI-powered operations management to optimize performance and improve efficiency.
- VMware Aria Operations for Logs: Faster troubleshooting with deep operational visibility and intelligent log analytics.

## Network Enhancements

### SDDC Group to Group Connectivity

Customers with multiple SDDC Groups can now interconnect their SDDC Groups in the same Organization with few clicks.

This benefits customers who have created separate SDDC Groups per AWS region and need to connect them without disrupting existing network traffic. SDDC Group to Group connectivity is established using the existing Transit Connect per region. Interconnected SDDC Groups can leverage their existing external connections to Direct Connect Gateway and/or AWS VPC and Transit Gateways.

This feature is available for all customers on supported AWS versions (starting from 1.18) for both new and existing Transit Connect deployments. Customers can configure the feature from VMware Cloud Console in SDDC Group UI by selecting desired SDDC Groups to connect.

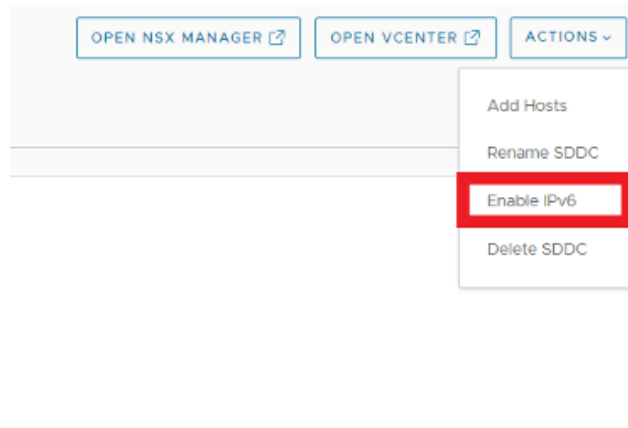
### NSX Alarms Improvements

The new version of NSX included with VMware Cloud on AWS SDDC version 1.24 introduces additional out-of-the-box alarm definitions available in the NSX Manager Console improving the troubleshooting and serviceability of the solution. You can find the new alarm definitions in the Alarms – Alarms Definitions tab. The new alarm definitions include LDAP connectivity, AD group membership change and IPAM-related alarms.

Feature	Event Type	Severity	Enable Detection	Create Alarms	Create SNMP Traps
Distributed Firewall	DFW CPU Usage Very High	Critical	Yes	Yes	Yes
Distributed Firewall	DFW Session Count High	Critical	Yes	Yes	Yes
Distributed Firewall	DFW Vmotion Failure	Critical	Yes	Yes	Yes
Distributed IDS IPS	NSX IDPS Engine Memory Usage High	Medium	Yes	Yes	Yes
Groups	Active Directory Groups Modified	Medium	Yes	Yes	Yes
Identity Firewall	Connectivity To LDAP Server Lost	Critical	Yes	Yes	Yes
IPAM	IP Block Usage Very High	Medium	Yes	Yes	Yes
IPAM	IP Pool Usage Very High	Medium	Yes	Yes	Yes

### Enhanced IPv6 Support

IPv6 protocol support has been introduced in VMware Cloud on AWS v1.22 and has been extended in the new 1.24 release. Previously VMware Cloud on AWS announced support for IPv6 communication over Direct Connect and VMware Transit Connect which allows to use of IPv6 workloads inside SDDC and workloads communication with on-premises datacenters. Customers have to enable IPv6 individually on each SDDC from the Actions menu at the SDDC Summary tab.



## Enable IPv6 (Dual Stack) ✕

You are enabling IPv6 support in this SDDC using AWS auto-assigned IPv6 addresses. IPv4 will continue to work in the SDDC. Once enabled, IPv6 cannot be disabled. [LEARN MORE](#)

CANCEL CONTINUE

With the 1.24 release IPv6 enabled VMs can now communicate with SDDC Management components such as vCenter (which is using IPv4) using NAT64 rules. If you require IPv6 workloads to communicate with SDDC Management components, work with your VMware representatives. You can learn more about IPv6 support on VMware Cloud on AWS by reading the following blog [Introducing IPv6 Networking in VMware Cloud on AWS](#).

## vSAN Express Storage Architecture

The most recent blog post [vSAN ESA now available in VMware Cloud on AWS](#) announces a new chapter in the evolution of VMware Cloud on AWS storage foundation and we will reveal some exciting details about it below.

VMware Cloud on AWS release 1.24 introduces vSAN Express Storage Architecture (ESA) which is supported on i4i.metal host type for new SDDCs. To enable vSAN ESA feature customers currently require assistance from the VMware team. To learn more about vSAN ESA architecture, please refer to [vSAN ESA Frequently Asked Questions](#).

vSAN ESA is a single-tier Hyper-Converged Infrastructure (HCI) solution designed to optimally leverage NVMe storage devices, providing performance and compression increase.

New vSAN ESA features such as native snapshots lead to faster backups, and a storage pool architecture reduces fault domains and improves data availability.

vSAN ESA architecture supports RAID5 Storage policy starting from 3 hosts that give customers more storage capacity on small clusters compared to vSAN Original Storage Architecture.

vSAN ESA is available for greenfield SDDC as primary and secondary clusters. Enabling vSAN ESA is a one-click selection during a new SDDC or cluster deployment. You can read more in the following article: [vSAN ESA with VMware Cloud on AWS: Technical Deep Dive](#)

### < Create Software-Defined Data Center (SDDC)

1. SDDC Properties Give your SDDC a name, choose a size, and specify the AWS region where it will be created.

**SDDC Name** VSAN ESA SDDC

**AWS Region** US West (Oregon)

**Deployment**  Single Host  Multi-Host  Stretched Cluster

**Host Type** i4i (Local SSD)

**vSAN ESA**  Enable

**Number of Hosts** 3

**Host Capacity** 2 Sockets, 64 Cores, 1 TiB RAM, 27.28 TiB Storage

**Total Capacity** 6 Sockets, 192 Cores, 3 TiB RAM, 81.85 TiB Storage

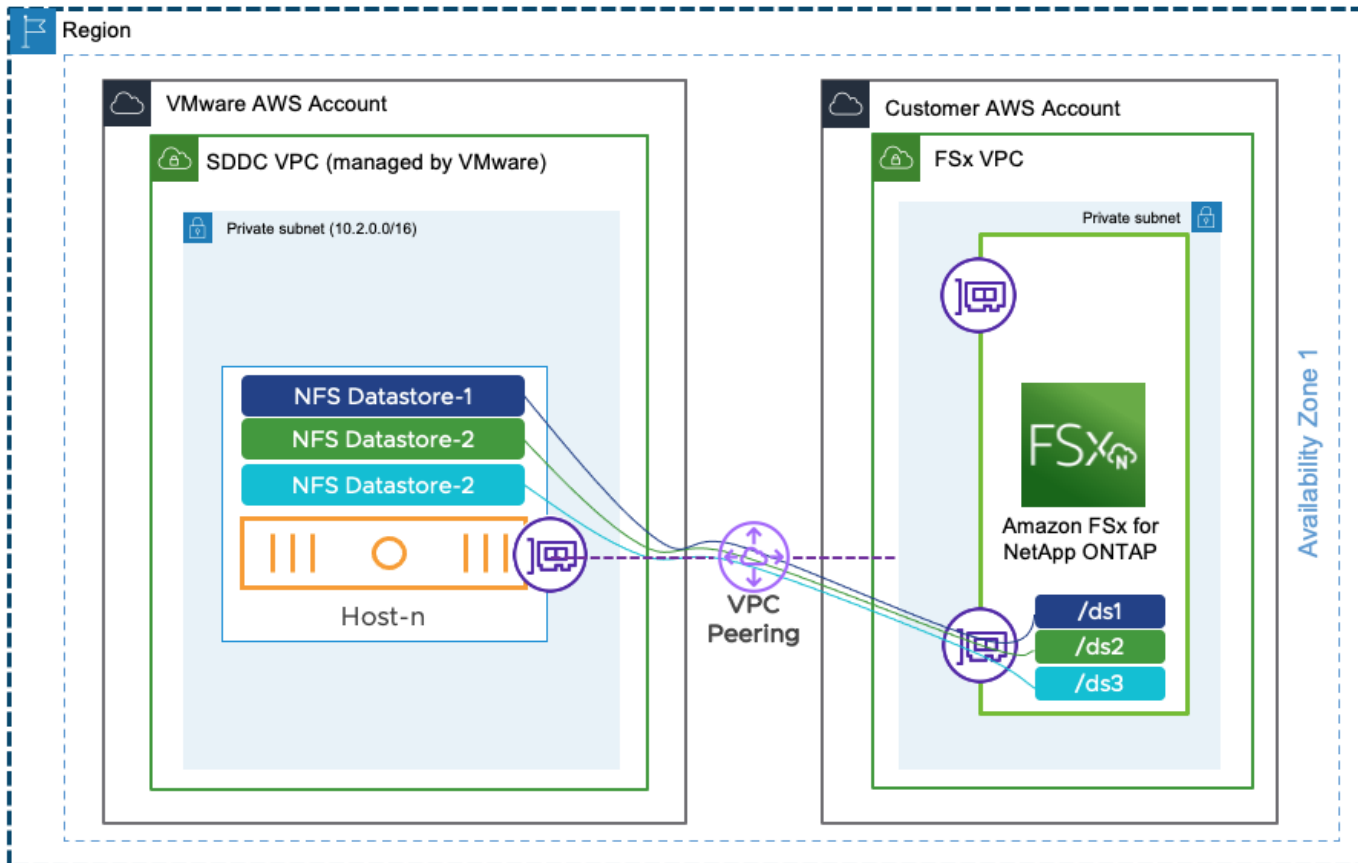
[SHOW ADVANCED CONFIGURATION](#)

[NEXT](#)

## External Storage Enhancements

### VPC Peering

This feature enables customers to establish a direct network link between their VMware Cloud on AWS SDDC and an Amazon VPC hosting Amazon FSx for NetApp ONTAP. This presents customers with a compelling network architecture, offering both simplicity and cost savings for external NFS storage. With the introduction of VPC Peering, customers can fully leverage the capabilities of Amazon FSx for NetApp ONTAP without incurring additional expenses associated with AWS Transit Gateway data processing fees.



To create VPC Peering, customers should initiate a VPC Peering request through their VMware Customer Success or Account team. For more details please read the [Feature Brief: VPC Peering](#).

### Increased NFS Performance

Using external NFS Datastores ([VMware Cloud Flex Storage](#) or [Amazon FSx for NetApp ONTAP](#)) introduces additional traffic flowing through the host network adapter. Using jumbo frames NFS storage traffic throughput can be significantly increased by reducing the overhead associated with transmitting NFS requests and responses. This can improve NFS performance, but all network devices in the path must support jumbo frames for it to be effective. SDDC version 1.24 for VMware Cloud on AWS supports increased MTU and would provide better performance for customers with External Storage.



## VMware Cloud Sizer

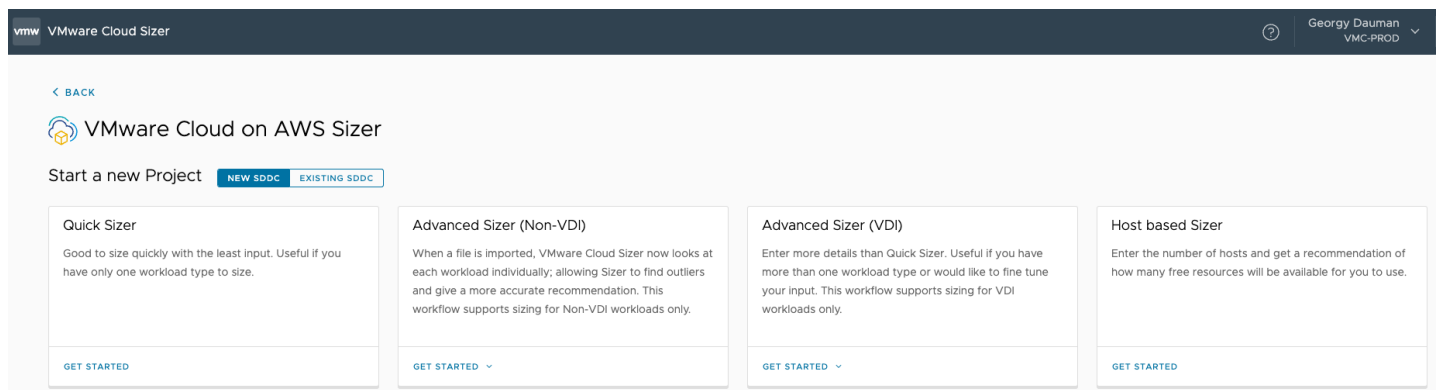
VMware Cloud sizer for AWS is going hand in hand with the new release of VMware Cloud on AWS and gets several new features and improvements.

First of all, it now features separate Advanced Sizer options for VDI and non-VDI workloads which segregates use cases and makes the sizing exercise more logical and simplified.

Secondly, an Advanced non-VDI sizer supports manual workload input in addition to RVTools and Live Optics import.

Introduction of Cluster Conversion Estimation allows for planning the migration of existing clusters in the SDDC to the latest host instances (e.g. conversion of i3 cluster to i4i).

Together with simplified profile settings, UI enhancements and Quick Sizer which now also supports external storage VMware Cloud Sizer becomes an even more handy tool making it essential for capacity planning.



You can explore all the capabilities of the Sizer by reading the [Feature Brief: VMware Cloud Sizer](#).

## Security Enhancements

There are a few enhancements added to version 1.24 further fortifying the security of VMware Cloud on AWS.

### Granular NSX Admin Roles

There are a few enhancements added to version 1.24 further fortifying the security of VMware Cloud on AWS.

Adding NSX Security Admin role to NSX adds granularity and enables separation of Security Admin and Network Admin roles for different teams of users. Granular role-based access control (RBAC) allows customers to assign limited access to Network-only or Security-only configuration on VMware Cloud on AWS, instead of providing full administration controls to the users.

Customers will now be able to configure four new roles for NSX Manager UI allowing users Full (Admin) or Read-only (Auditor) access to configurations respectively:

- NSX Security Admin
- NSX Security Auditor
- NSX Network Admin
- NSX Network Auditor

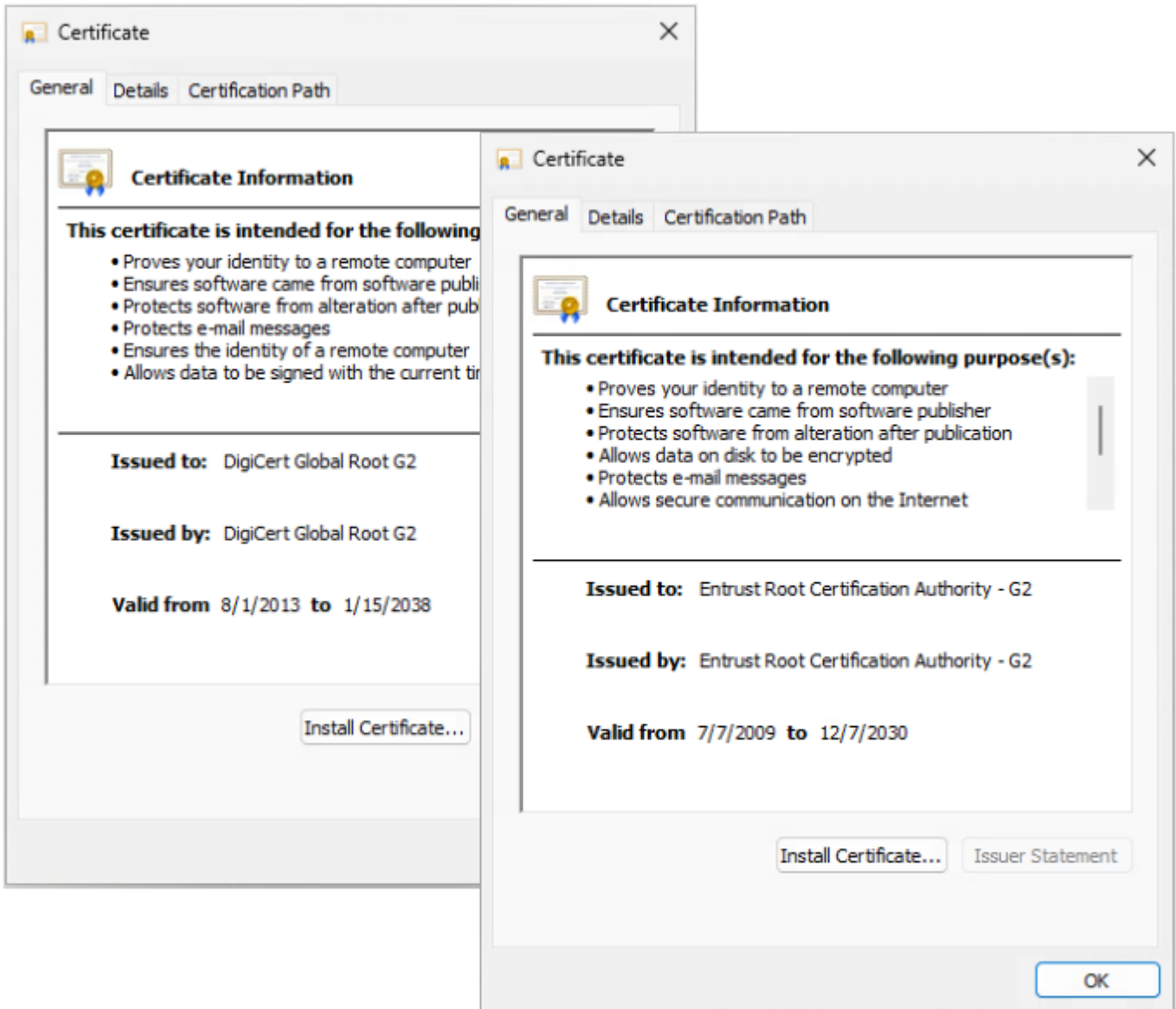
These new roles can be assigned by Organization Admin at the Identity and Access Management menu on the console.

The screenshot shows the VMware Cloud Services console interface. The left sidebar contains a navigation menu with categories like Services, Identity & Access Management, Billing & Subscriptions, Support Requests, Insights, Developer Center, and Organization. The 'Identity & Access Management' section is expanded, showing 'Roles' as the selected option. The main content area is titled 'IDENTITY & ACCESS MANAGEMENT Roles' and includes buttons for 'ADD ROLE', 'EDIT ROLES', and 'REMOVE ROLES'. Below these buttons is a table listing roles with columns for 'Role', 'Description', and 'Created by'.

<input type="checkbox"/>	Role	Description	Created by
<input type="checkbox"/>	NSX Network Admin	-	Built-in
<input type="checkbox"/>	NSX Network Auditor	-	Built-in
<input type="checkbox"/>	NSX Security Admin	-	Built-in
<input type="checkbox"/>	NSX Security Auditor	-	Built-in
<input type="checkbox"/>	Operations Administrator	VMware Aria Operations Administrator	Built-in
<input type="checkbox"/>	Operations ReadOnly	VMware Aria Operations ReadOnly	Built-in
<input type="checkbox"/>	Operations User	VMware Aria Operations User	Built-in
<input type="checkbox"/>	Organization Administrator	Organization administrators have limited administrative access	Built-in
<input type="checkbox"/>	Organization Member	Organization members hold the default organization role that	Built-in
<input type="checkbox"/>	Organization Owner	Organization owners have complete administrative access to t	Built-in

### New CA and TLS 1.3 Support

Support of DigiCert in addition to Entrust Certification Authority (CA) to issue SDDC certificates allows more reliable SDDC behavior during certificate renewals or SDDC upgrade operations.



SDDC version 1.24 introduces support for modern TLS 1.3 protocol for ESXi hosts. This protocol has lower latency, is more secure and complies with federal standards such as FIPS and NIST.

## Lifecycle Management Improvements

Lifecycle management in the new version of VMware Cloud SDDC got several enhancements such as non-disruptive vCenter certificate replacement and upgrade improvements making day 2 operations faster, more reliable and even less intrusive for the end users.

## Virtual Machine Hardware

SDDC version 1.24 now supports virtual machine compatibility ESXi 8.0 and later (vmx-20), and increases the default version for new VMs from ESXi 6.7 (vmx-14) to ESXi 7.0 U2 (vmx-19).

