

# Cisco ISE Performance, Scalability and Best Practices

Jesse Dubois - TAC Security Technical Leader BRKSEC-3234

cisco ivel

# Introduction



### About Jesse Dubois

job.jessedubois: 18 years in TAC

details.jessedubois:

Location: Durham, North Carolina Interests: Brewing, Golf, Cooking Pets: Dunkel, Apollo, Comet, Calypso Latest Travel: Brussels, Belgium





cisco live!

### Webex App

#### Questions?

Use the Webex app to chat with the speaker after the session

#### How

- Find this session in the Cisco Events mobile app
- 2 Click "Join the Discussion"
- 3 Install the Webex app or go directly to the Webex space
- Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until February 28, 2025.

cisco / illa



#### Session Abstract

In today's world of constant attacks, malware and Ransomware, its important to design, deploy and manage your network with an identity aware secure access platform. Cisco ISE plays a key role for many security solutions and is also one of the main pillars in the overall Cisco's Software defined Access Architecture.

This session will show you how to deliver scalable and highly available access control services using ISE for wired, wireless, and VPN from a single campus to a global deployment. Methodologies for increasing scalability and redundancy will be covered such as load distribution with and without load balancers, optimal profiling design, lessons learned from the trenches, as well as serviceability tips and tricks to help you gain optimal value and productivity from ISE.

Attendees of this session will gain knowledge on how to best design ISE to ensure peak operational performance, stability, and to support large volumes of authentication activity. Various deployment architectures will be discussed including ISE platform selection, sizing, and network placement. Cisco ISE also enables cross-platform network system collaboration across your IT infrastructure by using pxGrid to monitor security, detect threats, and set network policy. Manage assets, configuration, identity, and access. The session will go through such deployment considerations and common architectures.

#### Session Objectives

- How to choose the deployment design that works for you!
- · How to get the most out of your deployment.
- My Tips What we see in TAC/Escalation (Best Practices)
  - · Avoid commonly seen pitfalls.
- Not a session on configuration.
  - Will include links where appropriate to guides.



# Agenda

CISCO

- Deployment/Sizing
- Scaling ISE Services
  - Certificates
  - Network Devices
  - BlastRADIUS
  - Load Balancing
  - Profiling
  - External Databases
- MnT / Log Analytics

# Deployment / Sizing

cisco live!

### **ISE** Architecture

Standalone ISE





#### Policy Administration Node (PAN)

- Single plane of glass for ISE admin
- Replication hub for all config changes

#### Monitoring & Troubleshooting Node (MnT)

- Reporting and logging node
- Syslog collector from ISE Nodes

#### Policy Services Node (PSN)

- Makes policy decisions
- RADIUS / TACACS+ Servers

#### pxGrid Controller

Facilitates sharing of context



Single Node (Virtual/Appliance)		Multiple Nodes (Virtual/Appliance)
Up to <b>50,000</b> concurrent endpoints	3700	Up to <b>2,000,000</b> concurrent endpoints

cisco / ile

## **Deployment Options**

Small	Medium	Large
<ul> <li>All Personas on 2 nodes</li> </ul>	Maximum 8 nodes	<ul> <li>Maximum of 58 nodes</li> </ul>
<ul> <li>Optional 3<sup>rd</sup> node for:</li> <li>Dedicated PSN</li> </ul>	<ul> <li>PAN + MnT on same node</li> </ul>	<ul> <li>All personas on dedicated nodes.</li> </ul>
<ul> <li>pxGrid node</li> </ul>	PSNs on dedicated nodes	Up to 50 PSNs
<ul> <li>Health Check node</li> <li>3<sup>rd</sup> node does not increase scale, it is for redundancy and load sharing purposes only!</li> <li>         Image: A state of the state o</li></ul>	<ul> <li>pxGrid can be enabled on up to 2 nodes</li> <li>Dedicated with 4 PSNs</li> <li>Added to PAN + MnT</li> <li>Added to 2 PSNs</li> </ul>	
,		

cisco live!

#### Large Deployment: Centralized or Distributed



cisco /

•

#### Large Deployment: Separate Cubes



• RADIUS more latency tolerant then internode communication.

cisco (

•

### Latency Guidance

- Latency guidance is not a "fall off the cliff" number, but a guard rail based on what QA has tested.
  - 300ms can be ok
  - 150ms may be to much
- Profiler config is primary determinant in replication requirements.
- Higher auth/profiling rates may require lower latency.

#### **ISE Max Sessions**

Maximum Concurrent Active Sessions

- ISE Licensing counts active endpoint sessions
- RADIUS Accounting defines session Start & Stop events
- Sessions Start upon RADIUS Authorization
- Sessions Stop upon :
  1) Disconnect 2) Session Expiration 3) Idle Timeout

#### Table 3. Maximum Concurrent Active Sessions for Deployments

ahaha cisco	Products and Services	Solutions	Support	Learn	Partners			
/ Cisco Identity Service	a Engine / Compatibility Informati	on /						
Performan	ce and Scalab	oility Gu	uide fo	or Cis	sco Ide	entity Ser	vices En	gine
					Save	Translations	<b>Download</b>	Print
							Bias-I	ree Language
Contents Devices Disferent Types of Sizing Guidelines f Considerations for RADIUS Authentic TACACS + Authent Scenario - Specific Cisco ISE Deploym Cisco ISE SXP See Cisco ISE Network Cisco ISE Vertual M	minology Disco ISE Deployment or ISE Deployment Choosing a Deployment disc Rates authon Rates Authentication Rates ent Scale Limits ing e.pplances achine and Cloud Platforms							
Overview								
This document lists the	sizing guidelines for Cisco Ide	entity Services	Engine (Cisc	o ISE).				
Cisco ISE Node Tern	ninology							
A Cisco ISE node can pr dependent on the role a Table 1 Different Types	ovide various services based nd personas that a Cisco ISE of Cisco ISE Nodes	on the person node assumes	a that it assu i.	mes. The i	menu options	that are available th	rough the Admin p	ortal are

ypes of Cisco ISE Nodes
Node Type Description

A Cisco ISE node with the Administration persona allows you to perform all administrative operations and configurations on Cisco ISE. It serves as a single pane of glass for viewing all

Deployment	Cisco SNS 3595	Cisco SNS 3615	Cisco SNS 3715	Cisco SNS 3655	Cisco SN 375	S Cisco 5	o SNS 3695	Cisco SNS 3795
Large	500,000	Unsupported	Unsupported	500,000	750,00	0 2,00	0,000	2,000,000
Medium	20,000	12,500	75,000	25,000	150,00	0 5	0,000	150,000
Small	20,000	12,500	25,000	25,000	50,00	0 5	0,000	50,000
					Evaluation	Small Deployment	Medium Deployment	Large Deployment



Policy Administration node (PAN)

#### Steady State versus Peak Demand

- Must take into account transactions per second (TPS)!
- You will have a mix of static and mobile endpoints
- Some endpoints are always on with long (8+ hours) session expirations
- Usage patterns will cause regional and periodic ebbs, flows, and spikes
  - · Increased regional activity "follows the sun"
  - Wireless roaming spikes on the hour to change classrooms and meetings
- Mobile endpoints hibernate & roam causing a 3-10X+ larger load
- Misconfigured devices can have 100–1000X larger than average auth load Table 4. Maximum Concurrent Active Sessions for Different ISE Appliances Acting as PSNs

PSN Type	Cisco SNS 3595	Cisco SNS 3615	Cisco SNS 3715	Cisco SNS 3655	Cisco SNS 3755	Cisco SNS 3695	Cisco SNS 3795
Dedicated PSN (only PSN persona)	40,000	25,000	50,000	50,000	100,000	100,000	100,000
Shared PSN (multiple personas)	20,000	12,500	25,000	25,000	50,000	50,000	50,000

CISCO / Alle

### **ISF** Performance & Scale

- Deployment Types
- Maximum Concurrent Active Session
- Deployment Scale Limits
- Protocol Performance
- Scenario Performance
- Configuration Objects



11 11 11 Products and Services Solutions Support Learn CISCO

Support / Product Support / Security / Cisco Identity Services Engine / Compatibility Information

Performance and Scalability Guide for Cisco Identity Services Engine

	🛨 Download	Print
Contents		
Overview		
Cisco ISE Node Terminology		
Different Types of Cisco ISE Deployment		
Maximum Concurrent Active Endpoints for Different Deployments		
Cisco ISE Deployment Scale Limits		
RADIUS Performance		
TACACS+ Performance		
Cisco ISE Scenario-Based Performance		
Cisco ISE Hardware Platforms		
Overview		
This document lists the performance and scalability metrics for Cisco Identity Services Engine (Cisco ISE).		
Cisco ISE Node Terminology		

A Cisco ISE node can provide various services based on the persona that it assumes. The menu options that are available through the Admin portal are dependent on the role and personas that a Cisco ISE node assumes

Table 1. Different Types of Cisco ISE Nodes

Node Type	Description
Policy Administration node (PAN)	A Cisco ISE node with the Administration persona allows you to perform all administrative operations and configurations on Cisco ISE. It serves as a single pane of glass for viewing all administrative operations, condigurations, and contextual data. It synchronizes the configuration to the rest of the nodes in the deployment.
Policy Service node (PSN)	A Clsco ISE node with the Policy Service persona provides network access, posture, guest access, client provisioning, and profiling services. This persona evaluates the policies and makes all the decisions.
Monitoring node (MnT)	A Clicc ISE node with the Monitoring persona functions as the log collector and stores log messages from all the Administration and Policy Service nodes in a network. This persona provides advanced monitoring and roubleshooding tools that you can use to effectively manage the network and resources. A node with this persona aggregates and correlates the data that it collects, and provides you with meaningful reports.
pxGrid node	You can use Cisco pxGrid to share context-sensitive information from Cisco ISE session directory with other network systems such as Cisco ISE ecosystem partner systems and other Cisco platforms. The pxGrid framework can also be used to exchange policy and configuration data between nodes (like sharing tags and policy objects between Cisco ISE and third party vendors) and for other information exchanges.

#### **Different Types of Cisco ISE Deployment**



### Node Resource Profiles

Platform	Extra Small	Small	Medium	Large
Hardware	N/A	SNS-3715-K9	SNS-3755-K9	SNS-3795-K9
VMWare/Hyper-V/KVM	8 CPUs 32GB RAM 300GB Disk	24 CPUs 32GB RAM 300GB - 1.2TB Disk	40 CPUs 96GB RAM 300 GB - 1.2TB Disk	40 CPUs 256GB RAM 1.2TB - 2.4TB Disk
AWS	m5.2xlarge	c5.9xlarge* m5.8xlarge	m5.16xlarge	m5.16xlarge
Azure	Standard_D8s_v4	Standard_F32s_v2* Standard_D32s_v4	Standard_D64s_v4	Standard_D64s_v4
OCI	Optimized3.Flex (8 OCPU and 32 GB)	Optimized3.Flex (16 OCPU and 64 GB)* Standard3.Flex (16 OCPU and 128 GB)	Standard3.Flex (16 OCPU and 128 GB)	Standard3.Flex (32 OCPU and 256 GB)

\*This instance is compute-optimized and provides better performance compared to the general purpose instances.

Node is "profiled" each time it boots up, if profiles change resources are reallocated.

cisco

## Why Do Node Resource Profiles Matter?

- Internal Resources Allocated:
  - Java Heap Sizes
  - Oracle Memory Sizes
  - Thread Pool Sizes
  - Max Sessions
  - Etc...
- Virtual appliances mapped to physical profiles

Example: What we check: #Active profile properties [profile = sns3615, persona = pap\_mnt]

#### Profile differences:

<sns3615>.tomcat.runtimeThreadPool.maxThreads=200 <sns3755>.tomcat.runtimeThreadPool.maxThreads=300

Persona differences: <sns3615>.oracle.pga=1200 <sns3615>.<mnt>.oracle.pga=2400

### **ISE Platform Properties**

Verify ISE Detects Proper VM Resource Allocation

- From CLI...
  - ise-node/admin# show tech | begin "Displaying ISE Profile"

<pre>************************************</pre>	ISE Counte         From 2024-01-21 00:00:0         Filters: •         * Ser ·         * Time Ra ·	Prs 200.0 To 2024-01-21 10:29: NS_3615 * Is exactly (or	51.0 • isi • eq∨ • To	e-dunkel ∽ nday ∽
<ul> <li>From Admin UI</li> </ul>	Counter At	tribut <mark>e</mark> Thre	eshold	
<ul> <li>Operations &gt; Reports &gt;</li> </ul>	Attribute Name	ISE Profile	Threshold	
Diagnostics > ISE Counters > [node]	ARP Cache Insert Update	e R SNS_3615	95000	
(Under ISE Profile column)	DHCP Endpoint Detected	d SNS_3615	8000	
	DHCP Skip Profiling	SNS_3615	8000	
cisco (Ne!	BRKSEC-3234	© 2025 Cisco and/or i	its affiliates. All rights reserved. Cise	co Public 19

## Virtual Machine Resources

**Reservations/Features** 

- Applies to all virtual platforms VMWare, KVM, Hyper-V, AHV
- Reserve 100% of CPU and Memory
- Use thick provisioning of disk.
- Do no set resource limits.

CPU *	<u>12 v</u>
Memory *	<u>16384 MB ~</u>
Reservation	16384 MB ~
	Reserve all guest memory (All locked)
Limit	Unlimited 🗾 🗸 MB 🗸
Shares	Normal ~ 163840
Memory Hot Plug	Enable
> Hard disk 1	200 GB ~
SCSI controller 0	VMware Paravirtual
> Network adapter 1	VLAN_200 V
> Network adapter 2	VLAN_200 V

#### Virtual Machine Resources

#### Reservations – Before and After



cisco / ile

## Updated 3615/3715 (32GB) Node Guidance

- Small Deployments:
  - Recommend RADIUS or TACACS+ only workloads.
  - Log Analytics off by default, saves 2gb of memory.
  - Not recommended for AI/ML Profiling, ACI Integration, workload connectors.
- Medium Deployments:
  - Above applies if PAN/MNT nodes are 32GB memory nodes.
- Recommendation:
  - Use at least medium nodes (96GB memory) if advanced features are desired.
  - Apply latest patches for memory rebalancing changes.

# Virtual Machine Resources

- Do not set resource limits!
  - Resource requirements change between versions.

Virtual Machine Memory limit is lower than the allocated system memory

The VM Memory Limit is currently set to 16777216 kB and VM system memory is currently 32719416 kB.

When the VM Memory Limit is less than system memory, this can lead to the Application Server or OS crashing and not being able to recover on it's own.

Please verify that the VM memory limit is greater than or equal to the allocated system memory in the VM settings. If limit is unset that is also acceptable.

TAC Automation!

### Better Yet! Use the OVAs.

- Simplified for ISE 3.3
- Choose OVA based on Disk Size required.
- Will be prompted to choose node size needed.
- Reservations set automatically.

ISE 3.3 OVA file – 1200GB disk for Medium or Large with 37xx support (Recommend for PAN or MnT).

```
Cisco-vISE-1200-3.3.0.430a.ova
```

ISE 3.3 OVA file - 2400GB disk for Extra Large with 37xx support (Recommend for PAN or MnT).

### Cisco-vISE-2400-3.3.0.430a.ova

ISE 3.3 OVA file – 300GB disk for Eval, Small, Medium with 37xx support (Recommend for Evaluation, PSN or PxGrid).

```
Cisco-vISE-300-3.3.0.430a.ova
Advisories ⊡
```

ISE 3.3 OVA file – 600GB disk for Small or Medium with 37xx support (Recommend for PAN or MnT).

Cisco-vISE-600-3.3.0.430a.ova Advisories

### **Other Cautions**

- No snapshots!
  - Unable to quiesce database.
  - Use ISE Backup/Restore functionality for disaster recovery.
- Hot vMotion is supported.
  - Tested by System Scale and Test team.
  - TAC Experience:
    - Every environment is different, still some risk in losing the node.
    - Some risk in storage not re-attaching at they hypervisor level.
  - Safer to shut down the node and use cold vMotion.

# Scaling ISE Services





#### The Fall Out From the Mobile Explosion and IoT

- Explosion in number and type of endpoints on the network.
- High auth rates from mobile devices—many personal (unmanaged).
  - Short-lived connections: Continuous sleep/hibernation to conserve battery power, roaming, ...
- Misbehaving supplicants: Unmanaged endpoints from numerous mobile vendors may be misconfigured, missing root CA certificates, or running less-than-optimal OS versions
- Misconfigured NADs. Often timeouts too low & misbehaving clients go unchecked/not throttled.
- Misconfigured Load Balancers—Suboptimal persistence and excessive RADIUS health probes.
- Increased logging from Authentication, Profiling, NADs, Guest Activity, ...
- System not originally built to scale to new loads.
- End user behavior when above issues occur.
- Bugs in client, NAD, or ISE.



#### Turn Down the Firehose Multilayer Approach Rate Limiting at Source Filtering at Receiving Chain Detect and reject Count and discard Reauth period Heartbeat misbehaving clients Quiet-period 5 min repeated events frequency Held-period / Exclusion 5 min Log Filter Count and discard Switch untrusted events Load **Reauth phones** Balancer PSN MNT Quiet period ⇔∎ Unknown users WLC Ouiet Period LB Health Filter health Reject probes probes from $\infty \infty$ bad Roaming logging supplicant Count and discard supplicant **Client Exclusion** repeats and unknown NAD events Misbehaving supplicant

#### Let's Talk About Certificates

#### Top TAC Case Generator!







- Purchase Public Certificates!
- Don't train users to accept manin-the-middle attacks.



#### Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to **172.18.124.28**. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

#### What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using antivirus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

#### Learn more...

Go Back (Recommended) Advanced..





cisco live!



#### iPhones and Certificates Problem



### iPhones and Certificates

Problem







#### iPhones and Certificates Problem



### iPhones and Certificates

Problem







#### iPhones and Certificates Problem

• If users aren't looking at the phone:

Jun 05, 2019 10:57:56.269 AM	8	<u>o</u>	jfrost	EC:2C:E2:16:05:4A	5440 Endpoint abandoned EAP session and started new
Jun 05, 2019 10:57:05.726 AM	8	Q	jfrost	EC:2C:E2:16:05:4A	5440 Endpoint abandoned EAP session and started new

- Multiply this by hundreds of phones and multiple PSNs...
- Additionally, it is a poor end user experience.

#### Wildcard Certificates WildSAN or MultiSAN

Details		De
Issued To		lssu
Common Name (CN)	zer0k-ise.zer0k.org	Cor
Organization Unit (OU)	TAC	Org (OL
Organization (O)	Cisco	Org
City (L)	RTP	City
State (ST)	NC	Sta
Country (C)	US	Coι
Serial Number	42:00:00:00:0D:46:82:65:3D:42:C8:3C:CE:0 0:00:00:00:00:0D	Ser
Subject Alternative	DNS:zer0k-ise.zer0k.org,DNS:*.zer0k.org	Nar
Names		

#### tails ued To zer0k-ise.zer0k.org mmon Name (CN) TAC anization Unit Cisco ganization (O) Durham / (L) NC te (ST) US untry (C) 42:00:00:0E:A2:5A:BC:97:2A:E9:9A:9F:0 rial Number 0:00:00:00:00:0E DNS:zer0k-zer0k.org,DNS:isebject Alternative dunkel.zer0k.org,DNS:isemes maibock.zer0k.org,DNS:zer0kise1.zer0k.org,DNS:zer0k-ise2.zer0k.org
# WildSAN Security

- Certificate is valid for the entire domain:
  - Ex. zer0k.org
- If key is lost, cert could validate any site in the domain.

- Solution subdomain!
- · Deploy ISE in a subdomain:
  - Ex. ise.zer0k.org
  - · Limits validity of the certificate.
- Deploy MultiSAN
  - More expensive.
  - More difficult to expand deployment in future.

# Detour: Common Pitfall



cisco live!

Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
zer0k-wildsan	Admin, EAP Authentication		zer0k-ise.zer0k.org	zer0k-ca	Wed, 10 Jan 2024	Fri, 9 Jan 2026	~
							Active

- Problem.... Renew certificate but keep same CN
- ISE does not allow 2 certificates with same subject.
- Uploading cert with same subject replaces existing cert.
- Can't stage the certificate.
- Inconsistent replication of wildcard certs.

zer0k-ise.zer0k.org  $\overline{\Diamond}$ Issued By : zer0k-ca Expires : Fri, 9 Jan 2026 16:44:40 EST Certificate status is good Details Issued To Common Name (CN) zer0k-ise.zer0k.org TAC Organization Unit (OU) Cisco Organization (O) RTP City (L) NC State (ST) US Country (C) 42:00:00:00:0D:46:82:65:3D:42:C8:3C:CE:0 Serial Number 0:00:00:00:00:0D DNS:zer0k-ise.zer0k.org,DNS:\*.zer0k.org Subject Alternative Names

	Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
_	zer0k-wildsan	Admin, EAP Authentication		zer0k-ise.zer0k.org	zer0k-ca	Wed, 10 Jan 2024	Fri, 9 Jan 2026	
								Active

- Solution!
- The subject isn't just the CN, it is all of this!
- Change any 1 field and the subject is unique.

$\odot$	zer0k-ise.zer0 Issued By : ze Expires : Fri, 9	k.org r0k-ca 9 Jan 2026 16:44:40 EST	
Certific	ate status is go	od	
Details			
Issued To			
Common N	ame (CN)	zer0k-ise.zer0k.org	
Organizatio (OU)	n Unit	TAC	
Organizatio	n (O)	Cisco	
City (L)		RTP	
State (ST)		NC	
Country (C)	)	US	
Serial Number		42:00:00:00:0D:46:82 0:00:00:00:00:0D	2:65:3D:42:C8:3C:CE:0
Subject Alt	ernative	DNS:zer0k-ise.zer0k.c	org,DNS:*.zer0k.org



Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
zer0k-wildsan	Admin, EAP Authentication		zer0k-ise.zer0k.org	zer0k-ca	Wed, 10 Jan 2024	Fri, 9 Jan 2026	<ul> <li>Image: A set of the set of the</li></ul>
							Active

-= Prerequisite =-

- Ensure all nodes are in sync and not replicating slowly
- If CA certs have changed:
  - Upload them to ISE
  - Set them for "Trust for authentication within ISE" (admin) and/or "Trust for client authentication and Syslog" (EAP)

zer0 Issu Exp	zer0k-ise.zer0k.org Issued By : zer0k-ca Expires : Fri, 9 Jan 2026 16:44:40 EST				
Certificate s	itatus is good				
Details					
Issued To					
Common Name	(CN) zer0k-ise.zer0k.org				
Organization Ur (OU)	nit TAC				
Organization (O	)) Cisco				
City (L)	RTP				
State (ST)	NC				
Country (C)	US				
Serial Number	42:00:00:00:0D:46:82:65:3D:42:C8:3C:CE:0 0:00:00:00:00:0D				
Subject Alterna Names	tive DNS:zer0k-ise.zer0k.org,DNS:*.zer0k.org				

	Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	Status
_	zer0k-wildsan	Admin, EAP Authentication		zer0k-ise.zer0k.org	zer0k-ca	Wed, 10 Jan 2024	Fri, 9 Jan 2026	
								Active

-= Step1 =-

- Create a new CSR modifying the OU, O, L, ST, or C field.
  - OU tends to be the best candidate.
- Have CSR signed by CA.

bject		
Common Name (CN) ise.zer0k.org	0	
Organizational Unit (OU) TAC 2024	0	
Organization (O) Cisco	0	
City (L) RTP		
State (ST) NC		
Country (C) US		
🔛 DNS Name 💛 ise.	eer0k.org — 🕂	



zer0k-ise2024	Not in use	ise.zer0k.org	zer0k-ca	Mon, 22 Jan 2024	Wed, 21 Jan 2026	Active
zer0k-wildsan	Admin, EAP zer0k-wildsan entication	zer0k-ise.zer0k.org	zer0k-ca	Wed, 10 Jan 2024	Fri, 9 Jan 2026	Active

-= Step 2 =-

- Bind cert to CSR without choosing any roles.
- Log directly into each node and view the certificates page.
- Verify that the certificate has been successfully replicated to all nodes.
- If not:
  - ISE 3.2+, syncup nodes with missing certs.
  - ISE 3.1 or earlier, delete cert, fix nodes, try again -or- deregister nodes, install wildcard cert, reregister nodes.



zer0k-ise2024 Admin, EAP Authentication	ise.zer0k.org	zer0k-ca	Mon, 22 Jan 2024	Wed, 21 Jan 2026	Active
-= St	ep 3 =-		ise.zer0k.org issued By : zer0 Expires : Wed, : Certificate status is good	k-ca 21 Jan 2026 15:13:47 EST 1	
<ul> <li>Select desired roles <ul> <li>If admin is select</li> <li>ISE 3.3+ has sc</li> </ul> </li> <li>Test!</li> <li>Delete the old certified</li> </ul>	for certificate. ted all nodes will heduled restart fe	reboot. eature.	Details Issued To Common Name (CN) Organization Unit (OU) Organization (O) City (L) State (ST) Country (C) Serial Number Subject Alternative Names	ise.zer0k.org TAC 2024 Cisco RTP NC US 42:00:00:00:11:20:F6:40:A9:E 0:00:00:00:00:11 DNS:ise.zer0k.org,DNS:*.zer0i	6:63:0C:6B:0

cisco live!

# Network Device Recommendations

cisco live!

# Accounting Best Practices (Wired)

- Ensure that start and stop accounting is configured
- Keep interim accounting to a minimum
  - Inactive sessions are purged after 5 days

**Cisco Switches** 

sw# aaa accounting update newinfo periodic 2880



# Tune Wired NAD Configuration

#### Rate Limiting at Wired Source



Chart: Passed Authentications By Day

Failed Authentications Passed Authentication

· 802.1X Timeouts

- held-period: Increase to 300+ sec
- quiet-period: Increase to 300+ sec
- ratelimit-period: Increase to 300+ sec
- tx-period: 10 seconds
- Inactivity Timer: Disable or increase to 1+ hours (3600+ sec)
- Session Timeout: Disable or increase to 2+ hours (7200+ sec)

54

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

- Reauth Timer: Disable or increase to 2+ hours (7200+ sec)
- Bugfixes: Upgrade software to address critical defects.

BRKSEC-3234

# 9800 WLC

 Configure Interim-Accounting to send updates on new-info or roam only.



Configuration * > Security * > AA	A Show Me How 📀	
+ AAA Wizard		
Servers / Groups AAA Method Lis	AAA Advanced	
Global Config	Local Authentication	None 🔻
RADIUS Fallback	Local Authorization	None 🗸
Attribute List Name	Radius Server Load Balance	DISABLED
Device Authentication	Interim Update	
AP Policy	Interim Interval (Minutes)	2880
Password Policy	Show Advanced Settings >>>	
AAA Interface		

https://community.cisco.com/t5/security-knowledge-base/ise-and-catalyst-9800-series-integration-guide/ta-p/3753060

cisco /

# Use Fast BSS Transition (802.11r)

- Allow clients to roam without full 802.1x authentication.
- Supported by:
  - Apple Devices
  - Android Devices (platform and version dependent)
  - Some Windows devices (driver dependent)
- Clients that don't support 802.11r work on the same WLAN.
- TAC recommends over-the-air mode.



https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b wl 16 10 cg/802-11r-bss-fast-transition.html

## 9800 WLC Client Exclusions

Configuration * > Security * > Wireless Protection Polic					
Rogue AP Rules	Client Exclusion Policies				
	$\checkmark$				
Association Failures					
Authentication Failure	s 🔽				
Authentication Timeou	it 🗸				
IP Theft or IP Reuse					
uthentication Failures	$\checkmark$				
	Security • > Wirele Rogue AP Rules Association Failures Authentication Failures Authentication Timeou se uthentication Failures				

#### Configuration > Tags & Profiles > Policy

General	Access Policies	QOS and AVC	Mobility	Advanced
WLAN	Timeout			Fabrie
Session	Timeout (sec)	3600	(i)	Link-
Idle Time	out (sec)	300		mDN: Policy
Idle Thre	shold (bytes)	0		Hotsp
Client Ex	clusion Timeout (sec)	120		Use

cisco ile

# 9800 WLC Client Exclusions

**Tweaking EAP Timers** 

- $\cdot$  Clients excluded on
  - 6<sup>th</sup> 802.1x failure
  - 5<sup>th</sup> 802.1x timeout
- Advanced EAP timers should be tweaked to allow exclusion before client restarts.

Configuration						
EAP-Identity-Request Timeout (sec)*	5					
EAP-Identity-Request Max Retries*	5					
EAP Max-Login Ignore Identity Response	DISABLED					
EAP-Request Timeout (sec)*	5					
EAP-Request Max Retries*	5					
EAPOL-Key Timeout (ms)*	1000					
EAPOL-Key Max Retries*	2					
EAP-Broadcast Key Interval (sec)*	3600					



# Number of RADIUS Servers

- Keep it to 3 or less
- 3 retries at 5 seconds means 15 seconds per server.
- Devices won't wait long enough to make more worth while.
- More adds more chance for cascading failures.
- Need more? Add a load balancer!
- Use a **dead timer** of 10 minutes or more.
  - If all servers are exhausted the top server will be tried before the deadtime expires.

# BlastRADIUS



### BlastRADIUS – What is it?

- CVE-2024-3596
- Uses online MD5 prefix collisions to modify a RADIUS response
  - Example changing an Access-Reject to and Access-Accept
  - Must man-in-the-middle the RADIUS flow
- Can impact any Non-EAP RADIUS flow
  - EAP RFC Mandates the use of Message-Authenticator
- Utilizes the Proxy-State attribute to generate the collision gibberish



## Mitigation – End to End Encryption

- Radius over TLS (TCP) or RADIUS over DTLS (UDP)
  - ISE Supports DTLS today
  - Prevents Man-in-the-middle using strong, modern encryption
  - Provides full packet privacy
- Requires deployment and continued management of certificates on ISE and NADs
- Up to 15% performance hit for ISE authentication rate.
- IPSec can be used but is limited to 50 tunnels per PSN.

### Mitigation – Message-Authenticator

- Message-Authenticator
  - NAD must send it in all requests
  - Server must require it in all requests
  - Server must send it in all responses
  - NAD must require it in all responses
- ISE as a RADIUS Server can be configured per-above.
- ISE as a RADIUS Client: CSCwk67747
- 9800 sends and requires it with both 802.1x and MAC authentication
- IOS-XE sends and requires it with both 802.1x and MAC authentication





### **BlastRADIUS Resources**

- Cisco Security Advisory
  - <u>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-radius-spoofing-july-2024-87cCDwZ3</u>
- Mitigation Guide
  - <u>https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/222287-blast-radius-cve-2024-3596-protocol-sp.html</u>
- DTLS Configuration Example
  - <u>https://community.cisco.com/t5/networking-knowledge-base/configuring-radius-over-dtls-with-cat9k-and-ise-3-0/ta-p/4438427</u>

# Load Balancing

cisco live!

#### Load Balancing RADIUS, Web, and Profiling Services

- Policy Service nodes can be configured in a cluster behind a load balancer (LB).
- Access Devices send RADIUS and TACACS+ AAA requests to LB virtual IP.





# Traffic Flow–Fully Inline: VLAN Separation

Logical Network Separation Using Single LB Interface and VLAN Trunking



cisco / il

# Load Balancing Policy Services

#### RADIUS AAA Services

Packets sent to LB virtual IP are load-balanced to real PSN based on configured algorithm. Sticky algorithm determines method to ensure same Policy Service node services same endpoint.

#### Web Services:

• URL-Redirected: Posture (CPP) / Central WebAuth (CWA) / Native Supplicant Provisioning (NSP) / Hotspot / Device Registration WebAuth (DRW), Partner MDM.

No LB Required! PSN that terminates RADIUS returns URL Redirect with its own certificate CN name substituted for 'ip' variable in URL.

#### Direct HTTP/S: Local WebAuth (LWA) / Sponsor / MyDevices Portal, OCSP

Single web portal domain name should resolve to LB virtual IP for http/s load balancing.

#### • Profiling Services: DHCP Helper / SNMP Traps / Netflow / RADIUS

LB VIP is the target for one-way Profile Data (no response required). VIP can be same or different than one used by RADIUS LB; Real server interface can be same or different than one used by RADIUS

#### • TACACS+ AAA Services: (Session and Command Auth and Accounting)

LB VIP is target for TACACS+ requests. T+ not session based like RADIUS, so not required that requests go to same PSN

# Load Balancing RADIUS

#### Avoid spraying packets!!!



12953 Received EAP packet from the middle of conversation that contains a session on this PSN that does not exist

11051 RADIUS packet contains invalid state attribute

#### Load Balancing RADIUS IP vs Calling Station ID Stickiness



cisco / illa

# Load Balancer RADIUS Test Probes

#### **Citrix Example**

- Probe frequency and retry settings:
  - Time interval between probes:

interval seconds # Default: 5

Number of retries
 retries number

# Default: 3

Sample Citrix probe configuration:

add lb monitor PSN-Probe RADIUS -respCode 2 -userName citrix\_probe -password citrix123 -radKey cisco123 -LRTM ENABLED -interval 10 -retries 3 -destPort 1812

 Recommended setting: Failover must occur before RADIUS timeout (typically 15-35 sec) while avoiding excessive probing

#### F5 Example



- Time interval between probes:
   Interval seconds # Default: 10
- Timeout before failure = 3\*(interval)+1:Timeout seconds # Default: 31
- Sample F5 RADIUS probe configuration:

Name PSN-Probe Type RADIUS Interval 10 Timeout 31 Manual Resume No Check Util Up Yes User Name f5-probe Password f5-ltm123 Secret cisco123 Alias Address \* All Addresses Alias Service Port 1812 Debug No



# Load Balancer for ISE Best Practice Check List

- Persistence (Stickyness) is a must!
- Persistence based on Calling-Station-ID is best
- Avoid using Source-IP address for sticky value
- Sticky Timers need to be at least 1 hour
- DO NOT Round Robin Traffic
- Use the vendor specific guides from the community:

https://cs.co/ise-berg#load-balancing

# Profiling



# **Profiling Probe Selection Best Practices**

Probe	Key Profiling Attributes
RADIUS	MAC Address (OUI), IP Address, NDG values
RADIUS w/Device Sensor	CDP/LLDP, DHCP, User-Agent, mDNS, H323/SIP
RADIUS w/ACIDex	MAC Address (OUI), UDID, Operating System, Platform/Device Type
SNMP	MAC Address (OUI), CDP/LLDP, ARP tables
DHCP	DHCP
DNS	FQDN
HTTP	User-Agent
NetFlow	Protocol, Source/Dest IP, Source/DestPorts
NMAP	OS, Common and custom ports, Service Version Info, SMB & SNMP data
AD	Operating System and Version, AD Domain
pxGrid	IoT Asset, Custom Attributes
Endpoint Custom Attributes	Customer defined
	ISE Profiling Design Guide 🔗 cs.co/ise-profiling

cisco live

# Impact of Ownership Changes



# Endpoint Attribute Filter and Whitelist Attributes

Reduces Data Collection and Replication to Subset of Profile-Specific Attributes

- Endpoint Attribute Filter aka "Whitelist filter"
  - Disabled by default. If enabled, only these attributes are collected or replicated.

Profiler Configuration	Administration > System Settings > Profiling
* CoA Type: Reauth 👻	
Current custom SNMP community strings: •••••••••	Show
Change custom SNMP community strings:	(For NMAP, comma separated. Field will be cleared on successful saved change.)
Confirm changed custom SNMP, community strings: EndPoint Attribute Filter: I Enabled	(For NMAP, comma separated. Field will be cleared on successful saved change.)
Save Reset	

- Whitelist Filter limits profile attribute collection to those required to support default (Cisco-provided) profiles and critical RADIUS operations.
  - Filter must be disabled to collect and/or replicate other attributes.
  - Attributes used in custom conditions are automatically added to whitelist.

# **Device Sensor**

- Sends profiling via RADIUS Accounting
- Replaces Probes:
  - HTTP Probe
  - SNMP Probe
    - CDP/LLDP
  - DHCP Probe
- No additional load balancing considerations
- Supported on Cisco Catalyst Switches and WLCs

# Device Sensor (9800)

Configuration • > Wireless • > Wireless Global						
Default Mobility Domain *	default		Configuration • >	Tags & Profiles	> Policy	
RF Group Name*	default	General	Access Policies	QOS and AVC	Mobility	Advanced
Maximum Login Sessions Per User*	0	RADIUS Pr	ofiling			
Management Via Wireless	$\checkmark$	HTTP TLV	Caching			
Device Classification		DHCP TLV Caching				
AP LAG Mode						
Dot15 Radio		WLAN Lo	ocal Profiling			
Wireless Password Policy	None	Global State of Device Classification		Enabled	Enabled (i)	
		Local Subs	scriber Policy Name	BUILTI	N_AUTOCO.× 🗸	

cisco live!
## Profiling Endpoint Owner Directory

- Changes how endpoint ownership works
- Rather then new PSN taking ownership and transferring attributes to itself, queries current owner instead.
  - Reduces owner thrashing
  - Reduces data sent between nodes
- Administration -> System -> Settings -> Light Data Distribution

#### Endpoint Owner Directory

Enable the Endpoint Owner Directory (EPOD) feature to store the PSN FQDN of each MAC address connecting to ISE and replicate this data across the PSNs in a deployment. The EPOD is used for profiling service, disabling this option will use legacy Profiler owners directory.

Enable Endpoint Owner Directory

### **Endpoint replication**

- Endpoint replication has two channels, Jgroups and Redis (mesh)
- Remove redundant replication which was eating up resources
- Only impacts dynamically learned (profiled) endpoints
- Enabled by default after upgrade to ISE 3.3.
- Administration -> System -> Settings -> Endpoint Replication

#### **Endpoint Replication**

Enable or disable the replication of dynamically discovered endpoints across all Cisco ISE nodes by clicking the relevant radio button below. This feature does not impact statically configured endpoints. Endpoints imported from CSV files and guest and posture-enabled endpoints are automatically replicated across all Cisco ISE nodes.

O Replicate endpoints to all nodes ()

Disable endpoint replication to all nodes



Cancel

#### **ISE Profiling Best Practices**

#### General Guidelines for Probes

#### • HTTP Probe:

- Use URL Redirects instead of SPAN to centralize collection and reduce traffic load related to SPAN/RSPAN.
- Avoid SPAN. If used, look for key traffic chokepoints such as Internet edge or WLC connection; use intelligent SPAN/tap options or VACL Capture to limit amount of data sent to ISE. Also difficult to provide HA for SPAN.

#### DHCP Probe:

- Use IP Helpers when possible-be aware that L3 device serving DHCP will not relay DHCP for same!
- Avoid DHCP SPAN. If used, make sure probe captures traffic to central DHCP Server. HA challenges.

#### SNMP Probe:

- For polled SNMP queries, avoid short polling intervals. Be sure to set optimal PSN for polling in ISE NAD config.
- SNMP Traps primarily useful for non-RADIUS deployments like NAC Appliance-Avoid SNMP Traps w/RADIUS auth.

#### NetFlow Probe:

- Use only for specific use cases in centralized deployments–Potential for high load on network devices and ISE.
- pxGrid Probe:
  - Limit # PSNs enabled for pxGrid as each becomes a Subscriber to same data. 2 needed for redundancy.
  - Dedicate PSNs for pxGrid Probe if high-volume data from Publishers.

#### **ISE Profiling Best Practices**

- Whenever Possible...
- Use Device Sensor on Cisco switches & Wireless Controllers to optimize data collection.
- Ensure profile data for a given endpoint is sent to a single PSN (or maximum of 2)
  - Sending same profile data to multiple PSNs increases inter-PSN traffic and contention for endpoint ownership.
- Ensure profile data for a given endpoint is sent to the same PSN
  - Same issue as above, but not always possible across different probes
- Use node groups and ensure profile data for a given endpoint is sent to same node group.
  - Node Groups reduce inter-PSN communications and need to replicate endpoint changes outside of node group.
- Avoid probes that collect the same endpoint attributes
  - Example: Device Sensor + DHCP Probe
- Enable Endpoint Attribute Filter

## External Databases





101 BRKSEC-3234 © 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Policy Sets

- USE THEM!
- Group Like Rules:
  - Guest vs. Corporate SSID, MAB vs 802.1x devices, etc...
- Improves rule readability.
- Reduces configuration mistakes.
- Improves rule processing.
- Can be created based on any attribute available in initial RADIUS packet.



#### Authorization Best Practices

- Order conditions so internal attributes are matched before external attributes.
- Do not authorize MAC addresses against Active Directory
  - Why would this be a bad idea?
  - Use Network Access: AuthenticationIdentityStore to reduce external ID store lookups •
- Order rules from most used to least used

Ø	My Bad Rule	OR	<b>با</b>	zer0k.org·ExternalGroups EQUALS zer0k.org/Users/Engineering Airespace·Airespace-Wlan-Id EQUALS 2	* PermitAccess
0	My Good Rule		((1-	Airespace-Airespace-Wlan-Id EQUALS 2	*PermitAccess
o lit		AND	墨	zer0k.org·ExternalGroups EQUALS zer0k.org/Users/Engineering	

#### MS AD Sites and Services



## **DNS** Caching

- Active Directory is DNS Heavy!
- Enabled by default starting with ISE 3.3

From each node CLI: service cache enable hosts ttl 180

No.	Time	Source	Destination	Protocol	Length	Info		
1824	37.482898	172.18.124.26	172.18.124.23	DNS	121	Standard	query	<pre>0xc9c9 SRV _ldaptcp.Default-First-Site-Namesites.gcmsdcs.zer0k.org</pre>
1825	37.484022	172.18.124.23	172.18.124.26	DNS	313	Standard	query	response 0xc9c9 SRV _ldaptcp.Default-First-Site-Namesites.gcmsdcs.;
1840	37.687312	172.18.124.26	172.18.124.23	DNS	79	Standard	query	0xfa2f A zer0k-dc1.zer0k.org
1841	37.687312	172.18.124.26	172.18.124.23	DNS	79	Standard	query	0xfe2b AAAA zer0k-dc1.zer0k.org
1842	37.687640	172.18.124.23	172.18.124.26	DNS	135	Standard	query	response 0xfe2b AAAA zer0k-dc1.zer0k.org AAAA fd2f:624f:f359:c124:1eea:4
1843	37.687643	172.18.124.23	172.18.124.26	DNS	111	Standard	query	response 0xfa2f A zer0k-dc1.zer0k.org A 172.18.124.23 A 172.30.112.1
2097	41.767565	172.18.124.26	172.18.124.23	DNS	80	Standard	query	0xdd8a A ise-dunkel.zer0k.org
2098	41.767565	172.18.124.26	172.18.124.23	DNS	80	Standard	query	0x5a88 AAAA ise-dunkel.zer0k.org
2099	41.767909	172.18.124.23	172.18.124.26	DNS	137	Standard	query	response 0x5a88 AAAA ise-dunkel.zer0k.org SOA zer0k-dc1.zer0k.org
2100	41.767909	172.18.124.23	172.18.124.26	DNS	96	Standard	query	response 0xdd8a A ise-dunkel.zer0k.org A 172.18.124.20
2144	42.784260	172.18.124.26	172.18.124.23	DNS	80	Standard	query	0x9905 A zer0k-ise2.zer0k.org
2145	42.784260	172.18.124.26	172.18.124.23	DNS	80	Standard	query	0xc20e AAAA zer0k-ise2.zer0k.org
2146	42.784586	172.18.124.23	172.18.124.26	DNS	96	Standard	query	response 0x9905 A zer0k-ise2.zer0k.org A 172.18.124.28
2147	42.784586	172.18.124.23	172.18.124.26	DNS	137	Standard	query	response 0xc20e AAAA zer0k-ise2.zer0k.org SOA zer0k-dc1.zer0k.org
2810	55.026035	172.18.124.26	172.18.124.23	DNS	81	Standard	query	0x33c0 A ise-maibock.zer0k.org
2811	55.026035	172.18.124.26	172.18.124.23	DNS	81	Standard	query	0xc53e AAAA ise-maibock.zer0k.org
2812	55.026389	172.18.124.23	172.18.124.26	DNS	97	Standard	query	response 0x33c0 A ise-maibock.zer0k.org A 172.18.124.21
2813	55.026394	172.18.124.23	172.18.124.26	DNS	138	Standard	query	response 0xc53e AAAA ise-maibock.zer0k.org SOA zer0k-dc1.zer0k.org
3969	78.222560	172.18.124.26	172.18.124.23	DNS	80	Standard	query	0xaf3f A ise-dunkel.zer0k.org
3970	78.222560	172.18.124.26	172.18.124.23	DNS	80	Standard	query	0xde3c AAAA ise-dunkel.zer0k.org
3971	78.222960	172.18.124.23	172.18.124.26	DNS	137	Standard	query	response 0xde3c AAAA ise-dunkel.zer0k.org SOA zer0k-dc1.zer0k.org
3972	78.223423	172.18.124.23	172.18.124.26	DNS	96	Standard	query	response 0xaf3f A ise-dunkel.zer0k.org A 172.18.124.20

cisco/i

## AD Join Point and Authentication Domains

Connection	Allowed Domains	Passiv	elD Gi	roups	Attributes	Advanced Settings				
Use all Activ	Use all Active Directory domains for authentication (i)									
Enable Selecte	C Enable Selected 🗍 Disable Selected Q Show Unusable Domains									
Name	)	^	Authent	Forest		SID				
subz	er0.zer0k.org		NO	zer0k.or	g	S-1-5-21-2126304257-2360180230-2307				
zer0l	c.org		YES	zer0k.or	g	S-1-5-21-263584093-2727726975-78036				

- Trusted (intra-/inter-forest) domains automatically discovered from the Join Point.
- These are the domains with 2-way bidirectional trust with the Join Point.
- You can then select/deselect which one to use (all selected by default).
- Deselect domains not used by ISE.

#### **AD** Test Authentication



cisco / ila

#### **AD** Test Authentication

#### Test User Authentication \* Username jesse Kerberos \* Password ..... Authentication Type Lookup MS-RPC MS-RPC Authorization Data 🔽 Retrieve Groups **Retrieve Attributes** Test Authentication Result Groups Attributes **Different authentication types** Instance : Zer0k ISE node can be selected to run the test auth Authentication Result : SUCCESS Can provide group & attribute details if options are selected Authentication Domain : ZerOk.org : Jesse@zer0k.org User Principal Name **Millisecond Response Times** User Distinguished Name : CN=Jesse R. Dubois, CN=Users, DC=zer0k, DC=org : 6 Found. Groups Attributes : 40 Found. Authentication Time : 35 Ms. Groups Fetching Time : 11 Ms. Attributes Fetching Time: 6 Ms.

## **Domain Diagnostics**



cisco / illo

#### **Domain Diagnostics**

+ Run Te	ests $\checkmark$ Q View Test Details $\checkmark$ 🔺	Stop All Running Tests	← Reset Al	II tests to " Not Run"	
	Test Name	Join Point	Status	Result and Remedy	Started
	DNS A/AAAA record high level API	zer0k	☑ Success	Address record found	00:18:02 06.02
	DNS A/AAAA record low level API q	zer0k	☑ Success	Address record found	00:18:12 06.02
	DNS SRV record query (i)	zer0k	☑ Success	SRV record found.	00:18:12 06.02
	DNS SRV record size (i)	zer0k	☑ Success	SRV query size is under maximum limit of 4k.	00:18:12 06.02
	Kerberos check SASL connectivity t	zer0k	☑ Success	SASL connectivity test to AD was successful	00:18:12 06.02
	Kerberos test bind and query to RO	zer0k	☑ Success	ROOT_DSE was successfully reached	00:18:12 06.02
	Kerberos test obtaining join point T	zer0k	☑ Success	TGT was obtained successfully	00:18:12 06.02

cisco live!

#### **Active Directory Best Practices**

- Use Sites and Services to contact local domain controllers
- Use Allowed Domains to restrict negative lookups
- Dedicate Domain Controllers in high volume environments
- Enable DNS Caching on each node
- Test and Monitor for Request Latency
- Use Domain Diagnostics to ensure Active Directory health

## MnT / Log Analytics

cisco live!

## External Syslog

- Use IP address where possible
- Limit number of Syslog targets
- Limit log categories
- Logging is done directly from the PSNs

	zer0k_splunk	splunk.zer0k.org	514	UDP SysLog
0	zer0k_splunk_IP	172.18.124.23	514	UDP SysLog

cisco/

## **DNS** Caching

- Enabled by default starting with ISE 3.3
  - External SYSLOG with FQDN sends DNS request for every SYSLOG packet without it!

service cache enable hosts ttl 180





## Logging Suppression

#### Administration -> Settings -> Protocols -> RADIUS

RADIUS Settings			
Suppression & Reports UDP Ports	DTLS		
Suppress Repeated Failed Clients	S		
Suppress Repeated Failed Clients (j)			
Detect two failures within	5	i	Minutes
Report failures once every	15	(i)	minutes (15-60)
Reject RADIUS requests from clients w	ith repeate	d failure	es (j)
Failures prior to automatic rejection	5	(i)	(2-100)
Continue rejecting requests for	60	<u>(</u> )	minutes (5-180)
Ignore repeated accounting updates within	5	i	seconds (1 - 86,400)
Suppress Successful Reports			
Suppress repeated successful authentication	ions 🕕		
Authentication Details			
Highlight steps longer than	500	<u>(</u> )	milliseconds (500 - 10,000)

- Do not disable suppression on production deployments.
- If troubleshooting, disable on a per client basis.
- Protects the deployment!



#### Manual Collection Filters

#### Administration -> Logging -> Collection Filters

	isco Identity Se	ervices Engin	e		4	dministratio	n / System
н	Deployment	Licensing	Certificates	Logging	Maintenance	Upgrade	Health Ch
••• ** •• ** •• **	Log Settings Remote Logging Logging Catego Message Catalo Collection Filter	ı Targets ries g s	Collection F Collection * Status © Enall * Attribu MAC Ad * Value 00:11: * Filter T Bypass S Duration © 60	ilter List > New C on Filters oled ~ te dress 22:33:44:55 Suppression () Minutes	collection Filter		



#### **Keepalive Probes**

#### Failed Accepted

- IOS XE treats a failed authentication as alive
  - Some load balancers such as F5 and Netscalaer as well
- Can expect probe to always fail authentication
- Filter only failed so any passed can be audited
- Other devices may see failed as alive, must test

Status	^	Attribute	Value	Filter Type	Time left (in minutes)
Enabled		User Name	ios-probe	Filter Failed	Unlimited

#### **Keepalive Probes**

#### Passed Required

- If probe authentication must Pass
  - Use Local User
  - Prevents External Database slowness from impacting performance
- Filter Passed and Failed by Username

Status	$\sim$	Attribute	Value	Filter Type	Time left (in minutes)
Enabled		User Name	loadbalance-probe	Filter All	Unlimited

## Dedicated MnT

- Only supported in Large Deployment
- Disables all roles besides MnT
- Disables replication to node freeing up:
  - Disk I/O
  - CPU
  - Memory

✓ Monitoring		
Role		
SECONDARY	~	
Other Monitoring Node		
ise-dunkel	Dedicated Mat	×
Dedicated MnT ()	Dedicated MNT improves Monitoring node performance by disabling all other personas and services enabled on that node.This can be selected only after registering the	
	node in deployment	
> Policy Service		



#### Authentication Summary Report Passed/Failed Ratio



cisco ile

### Authentication Summary Report

Authentications By Identity Store

Identity Store	Passed	Failed	Total	Failed (%)	Avg Response Time (ms)	Peak response Time (ms)
Internal Endpoints	261263	0	261263	0	15.06	27355
zer0k.org	193777	794	194571	0.41	54	17916
Internal Users	25136	1	25137	0	27.5	2778
Guest Users	77	6	83	7.23	14.87	60

cisco lite

## Authentication Summary Report

Authentications By ISE Server

Server	Passed	Failed	Total	Failed (%)	Avg Response Time (ms)	Peak response Time (ms)
zer0k-ise1	114142	143	114285	0.13	17.03	50044
zer0k-ise2	69354	12697	82051	15.47	20.51	10009
zer0k-ise3	6531	51	6582	0.77	20.01	1551
zer0k-ise4	4331	0	4331	0	75.33	1128

cisco lite

#### Millisecond Timestamps in Live Logs

- Internal vs. External Latency
- Just because it isn't red doesn't mean it isn't impactful



	Steps		
	Step ID	Description	Latency (ms)
	11001	Received RADIUS Access-Request	
	11017	RADIUS created a new session	0
	11117	Generated a new session ID	1
	15049	Evaluating Policy Group	84
	15008	Evaluating Service Selection Policy	0
	15041	Evaluating Identity Policy	181
	15048	Queried PIP - Network Access.AuthenticationMethod	14
	15013	Selected Identity Source - Internal Users	60
Ø	24210	Looking up User in Internal Users IDStore - test1	509
	24212	Found User in Internal Users IDStore	3
	22037	Authentication Passed	0
	24715	ISE has not confirmed locally previous successful machine authentication for user in Active Directory	0
	15036	Evaluating Authorization Policy	1
	24209	Looking up Endpoint in Internal Endpoints IDStore - test1	0
	24217	The host is not found in the internal endpoints identity store	4
Ø	15048	Queried PIP - Radius.NAS-Port-Type	680
	15048	Queried PIP - Network Access.UserName	10
	15048	Queried PIP - IdentityGroup.Name	2
	15048	Queried PIP - EndPoints.LogicalProfile	5
	15048	Queried PIP - Network Access.AuthenticationStatus	0
	15016	Selected Authorization Profile - PermitAccess	2
	22081	Max sessions policy passed	0
	22080	New accounting session created in Session cache	0
	11002	Returned RADIUS Access-Accept	1

## Log Analytics

- Operations -> System 360 -> Log Analytics
- Available from ISE 3.1
- Enabled by default in ISE 3.3



Understanding your ISE deployment with C.L.A.R.K. (Cisco Log Analysis & Remediation Kiosk) BRKSEC-2897 CLUS 2023



https://www.ciscolive.com/on-demand/on-demand-library.html#/session/1686177803851001VeK2

cisco /

#### Log Analytics TPS / Auth to Accounting Ratio



cisco live!

#### Log Analytics Top Talkers



cisco live!

## Key Takeaways

- Adhere to Deployment and Node sizing guidelines to ensure proper resources are allocated.
- Leverage load balancers for scale, high availability, and simplifying network config changes.
- Use best practice network device configurations.
- Ensure external databases are responding efficiently.
- Don't overwhelm ISE with unnecessary information.
- Monitor for changes that increase requests to ISE.

## ISE Bar: A Webex Team Space for ISE @ eurl.io/#ryJFrhiBW



ISE Bar - A Team Space for ISE - Join https://eurl.io/#ryJFrhiBW Meet People (2328) Messages Content Meetings \$ 0 You 5/1/23, 8:22 AM 🖕 ISE Resources 🖕 This is our monthly reminder post of our many public ISE resources! Please review the resources below.

search the Internet and/or this webex space for answers to your question(s) *before* posting here. We have included our many vanity shortcut URLs because they are hopefully easy to remember when you need to find something or share it with someone via chats and emails.

- ★ 🍈 ISE Resources: https://cs.co/ise-resources 🍈
- ★ ISE Webinars: https://cs.co/ise-webinars : First week of every month!
- ★ ISE YouTube Channel: https://cs.co/ise-videos : ISE Webinar archive and more!
- ★ ISE Training: https://cs.co/ise-training : YouTube, Cisco Live, and more!
- ★ ISE Community: https://cs.co/ise-community | How to Ask The Community for Help
- ★ ISE Product Documentation : https://cs.co/ise-docs
- ★ ISE Performance & Scale: https://cs.co/ise-scale
- \* ISE Feedback, Feature Requests, & Enhancements: https://cs.co/ise-wish
- ★ ISE Licensing Send all Licensing questions to PM Sally Rattanaburee (salratta@cisco.com)
- ★ ISE Software Lifecycle Support Statement
- ★ ISE Deployment & Integration Guides by Vendor and Product : https://cs.co/ise-guides
- ★ How to Determine the Scale of an ISE Deployment

#### Fill Out Your Session Surveys



Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the 'Participant Dashboard'





## Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at <u>ciscolive.com/on-demand</u>.
  Sessions from this event will be available from March 3.

Contact me at: jedubois@cisco.com



## Thank you

cisco Live!



# GO BEYOND